

Exhibit A

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION**

CASE NO.: _____

IN RE APPLICATION OF OFER LEVIN AND GTI
GLOBAL INVESTMENTS LTD. FOR JUDICIAL
ASSISTANCE PURSUANT TO 28 U.S.C. § 1782

_____ /

**DECLARATION OF SHAI SHARVIT IN SUPPORT OF APPLICATION OF OFER
LEVIN AND GTI GLOBAL INVESTMENTS LTD. FOR JUDICIAL ASSISTANCE
PURSUANT TO 28 U.S.C. § 1782**

Shai Sharvit declares under the penalty of perjury as follows:

1. My name is Shai Sharvit. I am a partner in the law firm of Gornitzky & Co. in Israel. I am duly admitted to practice law in Israel (and in good standing with the Israel Bar Association), and have been practicing law, in Israel, continuously for the past 22 years. My practice focuses on domestic and international commercial disputes.

2. I make this declaration in support of Ofer Levin ("Mr. Levin") and GTI Global Investments Ltd.'s ("GTI") Application for Judicial Assistance Pursuant to 28 U.S.C. § 1782 (the "§ 1782 Application"). The information contained herein is within my personal knowledge except where otherwise noted.

3. Unless otherwise stated, the information described below is based on my review of the court papers filed in Israel, information provided to me by Mr. Levin, and my own personal knowledge in my role as counsel for Mr. Levin and GTI in the legal proceedings described below. I represent Mr. Levin and GTI in court cases that have been lodged in Israel in connection with an arbitration award issued as a result of arbitration proceedings between Mr. Levin, GTI, Edmund Shamsi ("Shamsi"), and other individuals and entities associated with Shamsi.

I. The Parties to the Israeli Proceeding to Vacate the Arbitration Award.

4. Mr. Levin is a businessman and the manager of GTI. Mr. Levin is a former Israeli citizen who now resides in Slovakia.

5. The following companies are controlled by Mr. Levin and were named as parties to the Israeli arbitration proceedings: GTI; GTI Global Trends Investments Ltd.; GTI Ltd.; Blue Mountain Contemporary Art Ltd.; O.L. Holdings SARL; Morro Structured Products Ltd.; Morro Enterprises Ltd.; Itacare Ltd.; Jerusalem Property Holdings Ltd.; Harvest Sarl; Global Sunrise Ltd.; Sadot Participacoes Eirele; Santiya Operational Management Services GmbH; GTI International Investments Ltd.; Run Securities Ltd.; Global Heavy Transportation Ltd.; GTI Growth Investments Ltd.; Securities Control Ltd.; GTI Capital Investments Ltd.; Wipplinger Administrative Management Ltd.; and GTI Global Investments Ltd. (Cyprus) (the “Levin Named Entities”).

6. Shamsi is a businessman and Israeli citizen who immigrated to and resides in the Southern District of Florida, United States. Shamsi made investments via GTI with Mr. Levin.

7. Shamsi’s relatives, Helen Shamsi, Joshua Shamsi, Penina Shamsi, Benjamin Shamsi, Emmet Shamsi, Shir Shamsi, Lavi Shamsi, and Leon Avraham Shamsi, also invested funds into GTI and were parties to the arbitration proceedings in Israel.

8. Back Bay Manor Associates Limited Partnership (“Back Bay Manor Associates”) is a company owned by Shamsi that was a party to the arbitration proceedings in Israel.

II. The Israeli Proceeding to Vacate the Arbitration Award.

A. Background and Claims.

9. On January 26, 2025, Mr. Levin and the Levin Named Entities moved to vacate the arbitration award and appellate arbitration award entered in the arbitration proceedings between Mr. Levin, the Levin Named Entities, Shamsi, his relatives, and Back Bay Manor Associates. A

true and correct copy of the Motion to Vacate Arbitration Award and Answer to the Respondents' Motion to Approve the Arbitration Award (the "Motion to Vacate") is attached as **Exhibit 1**.¹

10. The subject of the dispute between the parties centers on investments made with Mr. Levin into GTI. **Ex. 1** at ¶ 13. In 2011, Shamsi and his relatives transferred \$18.4 million USD as a financial investment in GTI,² which was managed by Mr. Levin. *Id.* at ¶ 14. In 2014, the United States enacted the Foreign Account Tax Compliance Act ("FATCA"), which required Shamsi, as a United States citizen, to report and pay taxes on his investment in the United States and also required GTI to report accounts it managed on behalf of United States citizens. *Id.* Mr. Levin became aware that Shamsi failed to report his investments in compliance with the FATCA and also refused to allow GTI to report his investments. *Id.* Thus, GTI had to remove Shamsi's funds from GTI. *Id.* Subsequently, in 2015, the parties entered into joint venture agreements for the establishment of a joint venture to invest in real assets (the "Joint Venture Agreements"). *Id.*

11. Disputes eventually arose between Shamsi and Mr. Levin due to Shamsi's concerns about the implications of the Joint Venture Agreements under United States inheritance laws. *Id.* This dispute led to Shamsi filing a complaint for fraud in the Southern District of Florida (Case No.: 9:17-cv-80372) on March 22, 2017. *See id.* In his complaint, Shamsi claimed that the funds that had been invested in GTI, and later transferred for investments in real assets, had in fact been given to Mr. Levin as a loan. *Id.*

¹ As set forth *infra*, the Proceeding to Vacate the Arbitration Award is being held behind "closed doors" pursuant to Israeli law. Therefore, concurrently with the filing of this § 1782 Application, Applicants are seeking an order allowing them to file Exhibit 1 under seal in this Court. Until such time as the Court rules on the Motion for Leave to File Documents Under Seal, Exhibit 1 is being omitted from this filing.

² On information and belief, Shamsi's transfer to GTI was made from a U.S. bank account held at J.P. Morgan Chase Bank, N.A. ("J.P. Morgan Chase").

12. Shamsi's claim was compelled to arbitration in Israel pursuant to an arbitration agreement between the parties. *Id.* at ¶¶ 5, 15. In the arbitration proceedings, Shamsi, his relatives, and Back Bay Manor Associates (collectively, the "Shamsi Parties") alleged, *inter alia*, that the Joint Venture Agreements were sham agreements whereby the parties allegedly agreed that Shamsi and his relatives' funds would continue to be managed as part of GTI, in contravention of the law, while Shamsi was committing tax and reporting offenses. *Id.* at ¶ 15.

13. The arbitration was conducted in Israel beginning in June 2018 through May 31, 2023, before the Honorable Judge (ret.) Avi Zamir, and an arbitration award was issued on September 26, 2023 (the "Arbitration Award"). *Id.* at ¶¶ 5, 15-16. The Arbitration Award, which rejected the majority of Shamsi and the Shamsi Parties' claims, established there was no proof that any loan agreements had been signed by the parties or that a minimal return had been promised on the investments. *Id.* at ¶ 16. However, the Arbitrator did accept Shamsi and the Shamsi Parties' argument that the Joint Venture Agreements were sham agreements. *Id.* The Arbitrator required Mr. Levin and the Levin Named Entities to pay the investment amounts that had been invested by Shamsi and his relatives according to the value of the investments as of June 30, 2016, plus interest. *Id.*

14. Mutual appeals were filed against the Arbitration Award. *Id.* at ¶¶ 6, 17. An appellate arbitration award was issued on November 16, 2024 (the "Appellate Arbitration Award"). The Appellate Arbitration Award did not disturb the factual findings in the Arbitration Award, including the finding that the Joint Venture Agreements were sham agreements that enabled Shamsi to make misrepresentations to United States tax authorities and to banks in order to conceal the investments into GTI that had not been duly reported under FATCA. *Id.* at ¶ 17. The Appellate Arbitrator denied the appeals in their entirety and concluded that, although the Joint Venture

Agreements were illegal agreements, the principal objective of the parties in signing the Joint Venture Agreements was to enable the continued investment of funds into GTI and, therefore, the illegality of the Joint Venture Agreements was not sufficient to fully revoke those agreements. *Id.*

15. Shamsi and the Shamsi Parties moved to amend the Appellate Arbitration Award and, on December 1, 2024, the Appellate Arbitration Award was amended. *Id.* at ¶ 6. Shamsi and the Shamsi Parties then moved for a second time to amend the Appellate Arbitration Award, and, on December 26, 2024, a second order was entered amending the Appellate Arbitration Award. *Id.*

16. On January 1, 2025, Shamsi and the Shamsi Parties filed a Motion to Approve the Arbitration Award in the action styled *Shamsi, et al. v. Levin, et al.*, Civil Action Number 3216-01-25 (the “Proceeding to Confirm the Arbitration Award”). *See id.* at ¶ 10.

17. On January 26, 2025, Mr. Levin and the Levin Named Entities filed the Motion to Vacate in the action styled *Levin, et al. v. Shamsi, et al.*, Civil Action Number 67464-01-25, pending in the District Court, Tel Aviv, Israel (the “Proceeding to Vacate the Arbitration Award”). The Proceeding to Confirm the Arbitration Award and the Proceeding to Vacate the Arbitration Award are being heard (and will be decided) together and are the Israeli Proceedings for which Mr. Levin and GTI seek this Court’s judicial assistance pursuant to 28 U.S.C. § 1782.

18. The Motion to Vacate is based on the illegal conduct of Shamsi and the Shamsi Parties that fundamentally undermined the arbitration proceedings in Israel. *Id.* at ¶¶ 18-19. During the course of the arbitration proceedings, Mr. Levin and the Levin Named Entities were all victims of electronic attacks via email. *Id.* at ¶ 19. These electronic attacks were determined to be phishing email attempts to hack into the computer systems of Mr. Levin and the Levin Named Entities in an attempt to, among other things, locate and steal personal data. *Id.* Mr. Levin and the Levin Named Entities suspected that Shamsi and the Shamsi Parties, and/or agents operating on their

behalf, were behind the attacks. *Id.* Mr. Levin raised this suspicion in an affidavit filed in the arbitration proceedings and contacted Shamsi and the Shamsi Parties in writing about the hackings. *Id.* at ¶ 20. Shamsi and the Shamsi Parties denied their involvement. *Id.*

19. Concurrently, Mr. Levin identified an additional attempt to hack his credit data information at the Bank of Israel. *Id.* at ¶ 21.

20. Upon discovering the cyber-attacks, Mr. Levin contacted an Austrian investigation agency and asked them to forward his complaint to the Federal Bureau of Investigations in the United States (“FBI”). In his complaint, Mr. Levin requested that the agencies investigate the actions of Shamsi and the Shamsi Parties and/or agents acting on their behalf. *Id.*

21. Parallel to these hacking incidents during the arbitration proceedings, similar electronic attacks were identified against the attorneys for Mr. Levin and the Levin Named Entities in Israel and abroad. *Id.* at ¶ 22.

22. On these bases, Mr. Levin and the Levin Named Entities filed a motion for temporary injunction on August 8, 2019, against Shamsi and the Shamsi Parties in the initial arbitration proceedings. *Id.* at ¶ 23. Shamsi and the Shamsi Parties opposed the motion for temporary injunction on jurisdictional grounds but, in their response, admitted that Shamsi hired private investigators to conduct an investigation into the affairs of Mr. Levin and the Levin Named Entities. *Id.* The Arbitrator concluded that he did not have jurisdiction to issue the injunction requested and, thus, the motion for temporary injunction was stricken without hearing the claims on their merits. *Id.*

23. There were additional phishing email attacks against Mr. Levin and the Levin Named Entities, and/or agents acting on their behalf, which led to a second motion for temporary injunction relating to those electronic attacks to be filed on October 15, 2020. *Id.* at ¶ 24. The

Arbitrator again dismissed the motion for lack of jurisdiction, without hearing the claims on their merits. *Id.*

24. Mr. Levin and the Levin Named Entities hired the Wizman-Yaar investigation company from Israel and Athena Intelligence SA from Switzerland to conduct a comprehensive investigation to uncover the identity of the party or parties responsible for the hackings and identify the information obtained during the hacking incidents. *Id.* at ¶ 25. The investigations led to the conclusion that there was an “extremely high degree of likelihood” (about 95%) that the phishing attacks were conducted by a hack-for-hire group carrying out a focused cyber-attack in accordance with orders from a client. *Id.* at ¶ 26. On information and belief, the original “work order” for the operation against Mr. Levin and the Levin Named Entities used the code name “New project: Ofer.” Mr. Levin’s first name is Ofer.

25. Specifically, the unequivocal conclusion of these investigations was that the hack-for-hire was carried out by BellTrox, an Indian hacker group of highly seasoned internet mercenaries whose employees have been accused (across the United States and elsewhere) of crimes derived from internet hackings into the United States, as well as international companies and businesses, in attempts to gain access to private data and/or to engage in acts of fraud. *Id.* at ¶ 27. Copies of the expert report of Mr. Jonas Rey,³ the Founder and Partner of Athena intelligence SA and Cryptos Aegis, and the expert opinion of Mr. Raphael Balulu, a cyber forensic researcher and computer forensic analyst at Wizman-Yaar, are attached hereto as **Exhibits 2 and 3**.⁴

³ The report of Mr. Jonas Rey is being filed in redacted form pending the Court’s ruling on the concurrently filed motion seeking leave to file certain documents under seal.

⁴ To avoid an unnecessarily voluminous filing, the appendices to the expert reports are omitted from this filing. If requested by the Court, those appendices will be available for *in camera* inspection.

26. The United States has been undertaking efforts to dismantle the types of hacking operations linked to BellTrox. **Ex. 2** at ¶ 21. BellTrox's founder, Sumit Gupta, is wanted by the FBI for his involvement in hack-for-hire operations. *Id.* And several other private investigators, including three individuals with strong ties to Israel, Mr. Aviram Azari, Mr. Eitan Arusy, and Mr. Amit Forlit (the "Investigators"), were recently arrested, and/or arrest warrants have been issued against them, by U.S. authorities. *Id.* These Investigators were involved in hack-for-hire operations utilizing the services of BellTrox. *Id.*; **Ex. 3** at ¶¶ 36-39.

27. BellTrox was able to commercialize its large-scale hack-for-hire operations through private investigators like the Investigators. **Ex. 2** at ¶ 23.

28. The Investigators also control or controlled companies that may have been used to enable their hack-for-hire operations (the "Investigator Entities"). These entities were uncovered via court filings in the United States District Court for the Southern District of New York relating to hack-for-hire operations involving the Investigators and the Investigator Entities (Case No.: 1:22-cv-08728). *See also id.* at ¶ 21; **Ex. 3** at ¶¶ 33-39.

29. The Investigator Entities known at the time of filing this Declaration include: Gam Kan Lo Roffe Shinaim, LLC; Kan Lo Roffe Shinnaim, LLC; and Global Impact Services, LLC.

30. Other known cyber-attacks carried out by the Investigators shared identical characteristics and methodology to the attack aimed at Mr. Levin and the Levin Named Entities. **Ex. 3** at ¶ 39. Thus, the § 1782 Application seeks discovery of communications with the Investigators and Investigator Entities, if any, relating to the hack-for-hire operation against Mr. Levin and the Levin Named Entities.

31. Further, the data and evidence uncovered during the investigations strongly suggested that Shamsi was linked to the cyber-attacks. **Ex. 2** at 3; **Ex. 3** at ¶ 55. Shamsi's

involvement in the hackings was evidenced by, among other things, (i) the absence of evidence indicating attacks on Shamsi's own email addresses; (ii) Shamsi hiring private investigators in connection with the arbitration proceedings; and (iii) the substantial evidence linking Shamsi or someone acting on his behalf to the hacking of one of Mr. Levin's email accounts. **Ex. 2** at ¶ 59.

32. Shamsi owns and controls entities in the United States, specifically in the Southern District of Florida, that are believed to have been used to orchestrate the cyber-attacks on Mr. Levin and the Levin Named Entities (the "Shamsi Entities"). All of the Shamsi Entities are found in the Southern District of Florida:

- a. Revivim, LLC is a Florida limited liability company with its principal place of business at 20295 NE 29th Place, Suite 201, Aventura, Florida 33180, and for which Shamsi is the sole Manager;
- b. Lenachalah, LLC is a Florida limited liability company with its principal place of business at 20295 NE 29th Place, Suite 201, Aventura, Florida 33180, and for which Shamsi is the sole Manager;
- c. Countryside Commons SWF, LLC is a Florida limited liability company with its principal place of business at 9045 La Fontana Blvd., Suite 105, Boca Raton, Florida 33434, and for which Shamsi is the sole Manager.
- d. Hagefen, LLC is a Florida limited liability company with its principal place of business at 9045 La Fontana Blvd., Suite 105, Boca Raton, Florida 33434, and for which Shamsi is the sole Manager; and
- e. Sigal Group Developments, LLC is a Florida limited liability company with its principal place of business at 50 SE Olive Way Boca Raton, Florida 33432, and, on

information and belief, is a company associated with Shamsi and/or one or more of the Shamsi Entities.

See Composite Exhibit 4 (Printouts of the Shamsi Entities' information as found on the Florida Department of State, Division of Corporations website available at www.sunbiz.org).

33. Mr. Levin and the Levin Named Entities have also recently discovered that not only were their computers hacked, but the computers of the Arbitrator, the Honorable Judge (ret.) Avi Zamir, were targeted in a phishing attack, and apparently hacked during the arbitration proceedings. **Ex. 1** at ¶ 28. Thus, it has now been revealed that the computers of Mr. Levin and the Levin Named Entities, their legal counsel, and the Arbitrator were attacked and hacked during the arbitration proceedings. *Id.* But, curiously, the computers of Shamsi and the Shamsi Parties were not hacked. *Id.*

34. Additionally, Shamsi's misconduct was not limited to orchestrating cyber-attacks on his opponents and the Arbitrator. Shamsi tried to bribe one of his witnesses, Adv. Yossi Shefit, an individual who dealt with Shamsi's tax affairs and other issues common to Mr. Levin and Shamsi, to provide a false affidavit in the arbitration proceedings in exchange for \$50,000 USD. *Id.* at ¶ 33. And an additional bribe was carried out relating to the testimony of Mr. Yoni Saltzman, a lawyer who served as Mr. Levin's consultant during the negotiations of the Joint Venture Agreements, who testified for Shamsi and the Shamsi Parties. *Id.* at ¶ 34. Mr. Saltzman was asked during cross examination if he received any monetary consideration from Shamsi for his testimony, to which he stated he had in fact received money in exchange for his testimony. *Id.* at ¶ 35. It was revealed through Shamsi's CPA that Mr. Saltzman received \$250,000 USD for his testimony in favor of Shamsi. *Id.*

35. Shamsi and the Shamsi Parties also threatened and harassed employees, witnesses, and potential witnesses during the arbitration proceedings. *Id.* at ¶ 37. There were explicit threats against Mr. Levin and his family members, including threats to involve the Ukrainian mafia to “investigate” Mr. Levin’s family relating to the issues disputed in the arbitration proceedings. *Id.* at ¶ 39. Additional motions for temporary injunctions were filed based on these threats and bribes, but those motions were also dismissed on jurisdictional grounds without being heard on the merits. *Id.* at ¶¶ 38-39.

36. Based on the above, the Motion to Vacate asks that the Israeli District Court vacate the Arbitration Award and Appellate Arbitration award under Sections 24(9) and 24(10) of the Israeli Arbitration Law. *Id.* at ¶¶ 11, 47, 55.

37. Under Section 24(9), a court may vacate an arbitration award if the content of the award is contrary to public policy. *Id.* at ¶ 55.

38. Under Section 24(10), the grounds for vacation of an arbitration award include instances of infringement of the principles of natural justice, circumstances that would have justified holding a retrial, or an act of fraud that had an impact on the arbitration award. *Id.* at ¶ 47.

39. Applying the above principles, and in light of the hackings, the bribing of witnesses, and the threats of bodily injury, Applicants have asked the Israeli District Court to vacate the Arbitration Award and Appellate Arbitration Award. *Id.* at ¶¶ 47-61.

40. Simultaneously with the Motion to Vacate, Mr. Levin and the Levin Named Entities filed a motion for the proceedings on the Motion to Vacate to be held behind closed doors to safeguard the privacy of the parties and third parties (legal counsel and the Arbitrator), given the nature of the information that may have been exposed in the hacking incidents, and in light of the potential damage that may occur from public exposure of these hackings or attempted hackings.

Id. at ¶¶ 31, 63. The motion for the proceedings to be held behind closed doors explicitly excludes any other proceedings between the parties, including this § 1782 application.

41. If the Motion to Vacate is granted, the Arbitration Award and Appellate Arbitration Award will be vacated.

B. Nature of the Foreign Tribunal.

42. The Proceeding to Vacate the Arbitration Award is pending in the District Court of Tel Aviv, Israel. The Israeli District Court is a civil court of first instance.

C. Character of the Proceeding to Vacate the Arbitration Award.

43. Mr. Levin and the Levin Named Entities filed the Motion to Vacate pursuant to the jurisdiction granted to the District Court under Israeli Arbitration Law, 5728–1968 (the “Arbitration Law”). The Motion to Vacate is filed pursuant to Section 23(b) of the Arbitration Law, which allows a party to object to the confirmation of an arbitration award only by filing a motion to vacate the award. The grounds for vacation under Sections 24(9) and 24(10) are claimed pursuant to Section 21a(c)(1) of the Arbitration Law, as the case deals with an appellate arbitration award.

44. The Proceeding to Vacate the Arbitration Award is civil in nature. The Motion to Vacate seeks declaratory relief vacating the Arbitration Award and Appellate Arbitration Award.

III. Current Status of the Proceeding to Vacate the Arbitration Award.

45. On January 1, 2025, Shamsi and the Shamsi Parties filed the Motion to Approve the Arbitration Award in the Proceeding to Confirm the Arbitration Award.

46. On January 26, 2025, Mr. Levin and the Levin Named Entities filed the Motion to Vacate together with a motion for the proceedings to be held behind closed doors in the Proceeding to Confirm the Arbitration Award. Consistent with Israeli Procedure, and specifically with Section

23(b) of the Arbitration Law, 1968, the Motion to Vacate was also filed under a separate case number to initiate the Proceeding to Vacate the Arbitration Award.

47. Shamsi and the Shamsi Parties have objected to the proceedings being held behind closed doors and have denied that Mr. Levin and the Levin Named Entities are entitled to the relief sought under the Motion to Vacate; however, the Court decided, on an interim basis, to issue an order for the Motion to Vacate to be held behind closed doors pending any other decision.

48. The matter will, therefore, proceed as follows: (1) Shamsi must file his response to the Motion to Vacate by March 13, 2025; and (2) a hearing has been initially set by the Israeli District Court for March 26, 2025, but may be postponed at the discretion of the Court. During this hearing, witness cross-examination is to take place, and subsequent proceedings may take place, at the discretion of the Court, including the presentation of additional evidence.

IV. The Need for Evidence from the § 1782 Application Respondents.

49. At this time, the § 1782 Application seeks evidence from: (a) Shamsi, (b) the Shamsi Entities; and (c) J.P. Morgan Chase relating to, *inter alia*, the hacking incidents that occurred during the arbitration proceedings, as discussed in Section II of this Declaration.

50. The documents and information that Mr. Levin and GTI seek to obtain through this § 1782 Application (the “Evidence”) are unavailable in Israel but are essential to support Mr. Levin and the Levin Named Entities’ claims in the Motion to Vacate.

51. More specifically, and by way of example, the § 1782 Application seeks the following categories of documents and information (including testimony):

- a. Evidence regarding the flow of funds from Shamsi to the Investigators, Investigator Entities, and/or BellTrox;

- b. Shamsi's communications with the Investigators, the Investigator Entities, and/or BellTrox;
- c. Transaction information from Shamsi's bank accounts at J.P. Morgan Chase, which are believed to have been used to make payments to the Investigators, the Investigator Entities, and/or BellTrox relating to the hackings during the arbitration proceedings;
- d. J.P. Morgan Chase's communications with Shamsi, or anyone acting on his behalf, regarding the transfer of funds to the Investigators and/or the Investigator Entities; and
- e. Shamsi's communications relating to electronic hackings that occurred during arbitration proceedings in Israel, including but not limited to instructions given by Shamsi to the Investigators; and
- f. Shamsi's FATCA filings during the years 2015 through 2018 and in 2024.

52. The Evidence will assist Mr. Levin and GTI in establishing that Shamsi coordinated and/or funded the hacking incidents carried out by BellTrox targeting Mr. Levin the Levin Named Entities, their attorneys, and the Arbitrator during the course of the arbitration proceedings in Israel.

V. Israeli Law.

A. Availability of Discovery in Israel.

53. The Israeli District Court has the ability to order parties to produce evidence in accordance with Section 2 of the Arbitration Procedures Regulations, 1968 and Section 57 of the Civil Procedure Regulations, 2018 (*see also* OMA (Tel Aviv District Court) 32579-07-12 **Uzi Golan v. Shlomo Peri** (Nevo 4.3.2013); OMA (Central District Court) 26802-08-17 **Rotem**

Amfert Negev Ltd. v. Siemens AG (Nevo 17.9.2018); OMA (Jerusalem District Court) 7337-08 **DRY v. Zohar HaChaim Association** (8.9.2013); OMA (Nazareth District Court) 110/08 **Kibbutz Ein Zivan Agricultural Cooperative Society Ltd. v. Ben Nun** (30.4.2009)), and the court will most probably receive the evidence if produced. But the district court cannot compel the parties to produce evidence that is under the control of third parties that are not parties to the Proceeding to Vacate the Arbitration Award and Proceeding to Confirm the Arbitration Award, and holds wide discretion whether to order discovery or not.

54. Specifically, other than through the issuance of letters rogatory to a United States Court, or through the use of some other applicable international convention, there is no method by which J.P. Morgan Chase or the Shamsi Entities could be compelled to produce documents or provide testimony in the Proceeding to Vacate the Arbitration Award.

55. With respect to Shamsi and entities under his control or management, including but not limited to the Shamsi Entities, the Israeli District Court has the authority to compel Shamsi to produce the same evidence in Israel, and the discretion to exercise or not that authority (*see* authorities cited in paragraph 53, *supra*).

B. Use of Evidence in Israel.

56. Under Israeli law, written affidavits or statements as well as photocopies of documents may be used as evidence in Israeli courts. Sections 15(a) (for written affidavits) and 41 (for photocopies of documents) of the Evidence Ordinance [New Version], 1971 (“Evidence Ordinance”) permit the use of these documents as evidence subject to certain procedural requirements. Therefore, all evidence (including documents and testimony) gathered through the § 1782 Application will constitute evidence, subject to general admissibility rules, that may be used in connection with the Proceeding to Vacate the Arbitration Award.

C. Receptivity of the Israeli Government to the § 1782 Application.

57. Israeli law does not contain any prohibition against the gathering of evidence outside of Israel. Yaniv Vaki, **Law of Evidence** (Vol. A, 2020), Chapter 7: *Admissibility of Evidence – Types of Evidence*. Israeli courts are not precluded from or restricted in accepting or relying on evidence gathered in other countries, such as the United States through 28 U.S.C. § 1782. *See id.* Israeli courts recognize the admissibility of evidence collected abroad, provided it meets the admissibility requirements of Israeli evidentiary law. To the best of my knowledge, there has not been any case in Israel where an Israeli court has rejected evidence gathered in the United States, either partially or merely on the grounds that it was gathered outside of Israel.

D. The § 1782 Application Will Not Circumvent Israeli Proof-Gathering Restrictions or Other Israeli Policies.

58. In general, all sources of evidence are acceptable in proceedings in Israel's district courts. The Evidence Ordinance explicitly allows for the gathering of testimonial evidence (witness testimony under oath) (Sections 1-2), documentary evidence (written records, contracts, and reports) (Chapter 2), hearsay evidence (admissible under specific exceptions) (Section 10), expert evidence (testimony from qualified professionals) (Section 20), and circumstantial evidence (indirect proof of facts) (Section 53), as well as public certificates or institutional records (such as bank statements) (Sections 32-36). The courts have broad discretion in assessing the relevance, weight, and admissibility of evidence, provided it is reliable, relevant, and lawfully obtained.

59. The rights of the parties in the Proceeding to Vacate the Arbitration Award to present evidence for the court's consideration are only limited by the above-mentioned evidentiary rules. Therefore, the Evidence to be gathered through the § 1782 Application will not violate Israeli law.

60. In my opinion, the § 1782 Application would not circumvent any of the applicable Israeli proof-gathering restrictions, mandatory legal norms, or other Israeli policies.

VI. Ongoing Proceedings in Israel.

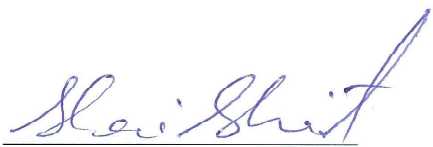
61. The proceedings currently pending in Israel – or anywhere, for that matter – involving Mr. Levin, GTI, and Shamsi are as follows:

- a. The Proceeding to Confirm the Arbitration Award (discussed *supra*);
- b. The Proceeding to Vacate the Arbitration Award, for which Mr. Levin and GTI seek discovery pursuant to 28 U.S.C. § 1782 (discussed *supra*);
- c. Attachment Proceedings initiated by Shamsi on October 15, 2023, pending in the Tel Aviv District Court in the action styled *Shamsi, et al. v. Levin, et al.*, Civil Action Number 21211-10-23; and
- d. Civil Claim initiated by Mr. Levin in January 2023, currently pending in the arbitration proceeding titled *Levin, et al. v. Shamsi, et al.*, Arbitration Case No. 981-109.

62. There may be other related proceedings in the future. If that is the case, I will supplement this Declaration.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: 03.09.2025


Shai Sharvit

ACTIVE:35679157.3

Exhibit 1

(Subject to concurrently filed
Motion for Leave to File
Exhibits Under Seal)

Exhibit 2

Expert Report

In the matter of Civil Proceeding 3216-01-25 Shamsi et al. v. Levin et al (and the related setting aside application)

This Expert Report was prepared at the request of Gornitzky & Co. law firm, in connection with the Civil Proceeding filed on January 1, 2025, by Mr. Edmund Shamsi ("**the Petitioner**" and/or "**Mr. Shamsi**") against Mr. Ofer Levin ("**the Respondent**" and/or "**Mr. Levin**"), to the District Court in Tel Aviv – Yafo, and the related setting aside proceeding.

This Expert Report is intended for submission to the court in the above proceeding, and I am well aware that for the purposes of the provisions of civil and criminal law in Israel regarding perjury, this written and signed Expert Report is considered as testimony under oath in court.

Expert name:

Mr. Jonas Rey, Swiss Passport No. X6464900

Location:

Geneva, Switzerland

Occupation:

Founder and Partner of Athena Intelligence SA and Cryptos Aegis

Education:

Master's Degree, International/Global Studies, University of Lucerne

Bachelor's Degree, Universite de Fribourg – Universitat Freiburg

Professional Experience:

As the Founder and current Partner of Athena Intelligence and its blockchain arm, SA and Cryptos Aegis, the largest Swiss based and regulated private intelligence and investigation Company, I have considerable experience investigating complex cyber incidents internationally. This includes investigations of hack-for-hire operations across the globe. Including the exposure of the infamous hackers' group BellTrox out of India, as part of the renowned Azima v. Rakia case.¹ I have

¹ J. Reddick, "American Businessman Settles Hacking Case in UK Against Law Firm," *The Record* (February 5, 2024), <https://therecord.media/american-businessman-settles-hacking-case-against-law-firm-uk>; *Ras Al Khaimah Investment Authority v Azima and Others* [2023] EWHC 2018 (Ch) ("**Azima v. Rakia case**").

contributed to multiple global investigations on the subject since then and my work has been pivotal in the global understanding of commercial hacking; and has been internationally recognized in a wide range of mediums e.g. the New Yorker and Reuters.²

I have previously served as the CEO of Liti Capital SA, the first blockchain based litigation finance company, before then becoming a Co-Founder and a member of the board of the company.

Before my career at Liti Capital SA, I served for over 7 years in Diligence Inc., managing complex cross-border investigations while developing the company's cyber intelligence practice. I began my career at Diligence Inc. as an analyst and finished as an Associate Partner.

Public Positions:

Vice President, Swiss Association of Intelligence and Investigation Practitioners

Licenses:

Athena Intelligence and Risk Management SARL is licensed by the Swiss Department of Foreign Affairs as a provider of corporate intelligence services, the license is attached as **Annex 1**.

Independence:

I have no personal connection to the Arbitration Proceedings (as defined herein) or any personal interest in the setting aside proceedings and/or their outcome.

I. Executive Summary

This Expert Report, prepared by Mr. Jonas Rey ("**the Expert**"), Founder and Partner of Athena Intelligence SA and Cryptos Aegis, provides a comprehensive analysis of the cyber-attacks related to the arbitration proceeding between Mr. Shamsi and Mr. Levin ("**the Arbitration Proceedings**"). The investigation was conducted at the request of Mr. Levin.

This Expert Report first examines the growing threat of hack-for-hire operations, which involve skilled hackers contracted to infiltrate specific targets for financial gain or competitive advantage and the significant risks these operations pose, particularly in high-stakes litigation and arbitration proceedings.

² D. Kirkpatrick, "A Confession Exposes India's Secret Hacking Industry," *New Yorker* (June 1, 2023), <https://www.newyorker.com/news/annals-of-crime/a-confession-exposes-indias-secret-hacking-industry>; R. Satter & C. Bing, "How Mercenary Hackers Sway Litigation Battles," *Reuters* (June 30, 2022), <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>.

The Expert's investigation identified BellTrox, an Indian-based hack-for-hire company, as a key player in these operations generally and as the most probable perpetrator of different hackings and hacking attempts on Mr. Levin's computers and the computers of others related to the Arbitration Proceedings (but not Mr. Shamsi).

The analysis involved examining the Tools, Techniques, and Procedures ("TTPs") used by the attackers in the specific hackings of Mr. Levin's computers. These TTPs were consistent with those documented in reports from third-party organizations and corroborated through interviews with former Belltrox employees involved in the hacking operations. The investigation also uncovered the use of phishing emails and advanced tracking technologies, to compromise sensitive information.

The Expert's Report concludes that BellTrox was likely contracted to carry out cyber-attacks targeting Mr. Levin, his legal representatives, and the arbitrator in the Arbitration Proceedings. The evidence suggests a potential link between the attacks and Mr. Shamsi, who may have ordered these efforts to gain leverage in the Arbitration Proceedings.

This Expert Report underscores the calculated and methodical nature of the attacks, which were executed with precision and intent. The findings provide an extremely high degree of probability in attributing the cyber-attacks to BellTrox.

II. General Background

1. In the digital age, the proliferation of cyber threats has become a formidable challenge for individuals, corporations, and governments alike. Cybersecurity breaches are no longer isolated incidents but are part of a broader, more insidious trend of **organized cybercrime**.
2. Within this realm, hack-for-hire operations have emerged as a significant threat. These operations involve skilled hackers who are contracted and offer their services to clients, often targeting personal and commercial sensitive information for financial gain or competitive advantage.

3. Such attacks can be profoundly damaging in today's interconnected world. A "successful operation" against a targeted individual or organization grants the attacker access to and even control over the target's most sensitive personal information—which may include bank accounts, government registry accounts, incriminating data, or private emails. This enables attackers not only to exploit the stolen information as such but also to weaponize it by threatening, coercing, or inflicting direct or indirect harm on the target and their network, including family members, colleagues, and associates.
4. The consequences of these operations can be severe when the targets are individuals or organizations in positions of significant influence—such as politicians, CEOs, judges, or arbitrators. One of the fields in which such nefarious operations have unfortunately become common is in support of litigation and arbitration proceedings, particularly where the stakes are high.³ The first instance of a large scale hacking in dispute resolution proceedings and arbitration was in 2015 as part of a large Kazakh dispute.⁴ Since then, there have been countless examples of hacked emails and hack-for-hire operations in dispute resolution proceedings, litigations and arbitrations aimed against parties, counsels and even judges and arbitrators.

III. Background to this Expert Report

5. I and Athena Intelligence SA more generally were instructed to carry out an expert analysis with respect to suspected cyber-attacks targeting Mr. Levin, his attorneys and other individuals involved in the Arbitration Proceedings between Mr. Levin (and certain corporate entities) and Mr. Shamsi (and additional individuals and corporate entities) ("**the Parties**").

³ C. Bing, "How Mercenary Hackers Sway Litigation Battles," *Reuters* (June 30, 2022); J. Stubbs, R. Satter & C. Bing, "Exclusive: Obscure Indian Cyber Firm Spied on Politicians, Investors Worldwide," *Reuters* (June 27, 2020), <https://www.reuters.com/article/technology/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUSKBN23G1F1>; D. Ziyaeva & A. Celso Pugliese, "Hacking the System: Admissibility of Evidence from Cyberattacks in Arbitration," *Global Arbitration Review* (July 19, 2024), <https://globalarbitrationreview.com/review/the-arbitration-review-of-the-americas/2025/article/hacking-the-system-admissibility-of-evidence-cyberattacks-in-arbitration>; R. Calvillo Ortiz, "Admissibility of Hacked Emails as Evidence in Arbitration," *Transnational Notes* (May 14, 2018), <https://transnational.law.nyu.edu/2018/05/admissibility-of-hacked-emails-as-evidence-in-arbitration/>; D. Croft, "Clive Palmer-Owned Company Accuses Government of Hacking Its Lawyers During \$300bn Lawsuit," *Cyberdaily* (February 13, 2024), <https://www.cyberdaily.au/security/10175-clive-palmer-owned-company-accuses-government-of-hacking-its-lawyers-during-300b-lawsuit>.

⁴ A. Ross, "Tribunal Rules on Admissibility of Hacked Kazakh Emails," *Global Arbitration Review* (September 22, 2015), <https://globalarbitrationreview.com/article/tribunal-rules-admissibility-of-hacked-kazakh-emails>.

6. Based on the information available to Mr. Levin, including findings from a subsequent investigation summarized in a report issued by Wizman Yaar Intelligence & Investigations⁵ ("WY" and "WY Report" respectively), he, his attorneys and other associated individuals were targeted by cyber-attacks.
7. In light of this information, it was suspected that these cyber-attacks were related to the ongoing dispute and subsequent Arbitration Proceeding, which is now the subject of these court proceedings.
8. I was therefore instructed by Mr. Levin to conduct a further investigation into these cyber-attacks to better understand, based on forensic and other evidence, whether these targets were specifically targeted and were therefore connected to the Arbitration Proceeding.

IV. Overview of My Investigation

9. My analysis involved examining the TTPs used by known cybercriminal groups. TTPs are the specific methods employed by cybercriminals to achieve their objectives and understanding them is crucial in order to be able to attribute them to a particular group or company. Similar to other criminal activities, every perpetrator has its own TTP and identifying these TTPs indicates which group of cyber-attackers is behind each specific attack.
10. In order to carry out my investigation which forms the basis of this Expert Report, I was provided with the following documents:
 - a. WY Report.
 - b. Emails received from Mr. Levin identified as Phishing Emails.⁶
 - c. Other related documents.
11. In addition, I had several discussions with lawyers from Gornitzky & Co. which provided me with additional information relating to the Arbitration Proceedings.

⁵ Wizman Yaar Investigations Report, of January 25, 2025 ("WYR"), attached as **Annex 2**.

⁶ Listed in the Athena Intelligence Intermediate Report, of January 19, 2024 ("AIR"), pgs. 7-15, attached as **Annex 3**.

12. At my request, Mr. Levin shared multiple phishing emails that he, his employees, his attorneys and others associated with him received between the summer of 2017 and the end of 2018. These emails are suspected to be part of the cyber-attacks related to the Arbitration Proceeding. I was also given additional email addresses linked to the Arbitration.
13. In addition, I was provided with information relating to approaches to Mr. Levin and his attorneys by Citizen Lab⁷ and Reuters⁸. Importantly, I was informed that Mr. Levin was contacted by Mr. Raphael Satter ("**Mr. Satter**"), a known Reuter's reporter who covers cybersecurity.⁹
14. Mr. Satter made an unsolicited approach to Mr. Levin and informed him that he was the victim of cyber-attacks of a hack-for-hire group whose data was compromised and shared with Reuters:

*"This is Raphael Satter; I am a reporter with the Reuters news agency. I'm getting in touch to warn you that hackers tried to break into your account & to ask for your help...Because these hackers often get involved in **legal battles, business disputes, and corporate espionage**, it is possible that your data was put at risk. I'd like to speak to you as soon as possible to brief you in further detail about what happened."*
15. Additionally, Mr. Levin's Lawyers were approached by Citizen Lab¹⁰, a global cyber investigation NGO working out of the University of Toronto in Canada, which were the first to expose the hacking group known as Belltrox (which I will discuss in this report) in the early months of 2020.
16. Based on this information, I conducted a comprehensive forensic investigation, which included an in-depth analysis of the evidence, interviews, and extensive research, which will be set out below.

⁷ The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security (<https://citizenlab.ca/about/>) – the relevant correspondence with Citizen Lab on June 13, 2020, is attached as **Annex 4**.

⁸ Reuters is the world's largest multimedia news provider (<https://www.reutersagency.com/en/about/reuters-about-us/>); the relevant correspondence with Reuters on April 8, 2021, is attached as **Annex 5**.

⁹ <https://www.reuters.com/authors/raphael-satter/>.

¹⁰ Annex 4.

V. BellTrox and Dark Basin - General

17. As I reference in my introduction, hack-for-hire operations are characterized by their professional approach, where hackers are contracted to infiltrate specific targets, often for corporate espionage or personal vendettas, as well as in the context of high-stakes disputes.
18. As noted above, over the past several years, I have spent a considerable amount of time investigating hack-for-hire operations across the globe. One of the groups which I exposed is a large network of hackers out of India.¹¹ One of these hacker groups operates under the name of Belltrox.¹²
19. These hack-for-hire operations are sometimes more difficult to investigate due to the fragmented structure of the hacking firms and teams. In some cases, the hacking instructions are given to several hackers and not just to a single employee and/or company which may use different tools and "TTRs" (Time to Remediate in cybersecurity is the amount of time it takes to fix a problem after it has been discovered), and therefore they might be more difficult to investigate.
20. Furthermore, this also means that even with respect to known hack-for-hire operations, the real scope and magnitude of the hacking might be significantly wider and more robust than the forensic evidence we are able to uncover.
21. BellTrox was founded by an individual named Sumit Gupta, who is wanted by the FBI since 2015 for his involvement in hack-for-hire operations.¹³ In its effort to dismantle these type of hacking operations, the US authorities have recently engaged in arrests of former Israelis who work as private investigators in the US and which used BellTrox extensively, such as Mr. Aviram Azary ("**Mr. Azary**"), Mr. Eitan Arusy and Mr. Amit Forlit.¹⁴

¹¹ J. Reddick, "American Businessman Settles Hacking Case in UK Against Law Firm," *The Record* (February 5, 2024); Azima v. Rakia case.

¹² *Dark Basin*, Wikipedia, https://en.wikipedia.org/wiki/Dark_Basin.

¹³ U.S. Attorney's Office, Northern District of California, "Private Investigators Indicted in E-Mail Hacking Scheme," (February 11, 2015), <https://www.justice.gov/usao-ndca/pr/private-investigators-indicted-e-mail-hacking-scheme>.

¹⁴ U.S. Attorney's Office, Southern District of New York, "Israeli Hacker-for-Hire Sentenced to 80 Months in Prison for Involvement in Massive Spearphishing Campaign," (November 16, 2023), <https://www.justice.gov/usao-sdny/pr/israeli-hacker-hire-sentenced-80-months-prison-involvement-massive-spearphishing>; R. Satter, "Israeli Accused of Hacking Released by UK Authorities Due to Misunderstanding," *Reuters* (May 9, 2024), <https://www.reuters.com/world/uk/israeli-accused-hacking-released-by-uk-authorities-due-misunderstanding-2024-05-09/>.

22. Typically, one side of a dispute would, generally through its lawyer, hire an investigator who would in turn hire an Indian hack-for-hire firm. The firm would then pass the hacked data back to the investigators who would either provide it to the lawyers as a tool (who then for example, could have access to the strategy of the opposing party in advance) or would leak said hacked emails to be able to state at a later conjecture that they had randomly stumbled upon them, which would allow the lawyers to submit them as evidence.¹⁵
23. BellTrox is one of the first firms that commercialized large scale commercial hack-for-hire operations. It marketed its services through private investigators who then resold them to lawyers and ultimately clients. BellTrox operated globally, but the most prominent area of its market was servicing clients in North America, through the network of Mr. Azary. At its peak, BellTrox consisted of a 20+ teams of social engineers and hackers supported by a network of ad-hoc consultants. The company allowed other hack-for-hire companies to use part of its infrastructure and it only stopped its operations in 2021 when the company was exposed through multiple press articles. Dark Basin is the name initially allocated by Citizen Lab to Belltrox and other hack-for-hire companies before Citizen Lab and other investigative entities, including myself, were able to provide a clearer picture of the companies and of the individuals involved.
24. My investigation with regards to this Expert Report identified BellTrox, as a key player in this domain. Belltrox's operations were meticulously executed, leaving behind Indicators of Compromise ("IOCs")—digital traces that help identify the perpetrators and are the most common TTR used to identify hackers. These IOCs were consistent with those documented in a report, titled, "Phish for the Future" by the Electronic Frontier Foundation ("EFF")¹⁶, which Citizen Lab later attributed to BellTrox:

*"Dubbed Dark Basin in a report into the group released today by The Citizen Lab, the group is tied to Indian company **BellTrox InfoTech Services Pvt Ltd**. It's believed to have targeted advocacy groups and journalists, elected and senior government officials, hedge funds and multiple industries".¹⁷*

¹⁵ J. Uchill, "Hack-and-Leak for Hire Being Sold as Litigation Assistance," *SC Media* (November 16, 2021), <https://www.scworld.com/analysis/hack-and-leak-for-hire-being-sold-as-litigation-assistance>.

¹⁶ E. Galperin & C. Quintin, "Phish for the Future," *EFF* (September 27, 2017), <https://www.eff.org/>.

¹⁷ C. Rothe, "'Dark Basin' Hacking Group Targeted Thousands in Hack-for-Hire Scheme," *Red Canary*, <https://redcanary.com/company/origin-story/>.

25. Additionally, it is important to highlight that direct hacking represents the final step in a much broader process of investigation and analysis of the targets. Groups like BellTrox follow strict protocols and initiate their attacks by gathering information from the “dark web” (the dark web refers to a hidden part of the internet accessible only through specialized software, like "Tor", where users can browse anonymously and access encrypted websites often associated with illegal activities or privacy-focused communication).¹⁸ This involves identifying sensitive information, such as passwords, browsing histories and personal data that is already publicly available or partially exposed.
26. Only after such information is harvested from the dark web, will the hackers move on to specifically hack the target, armed with the information they already found on the dark web. To the best of my knowledge, BellTrox used the same protocols and therefore, harvested information on the dark web for each and every one of its targets.
27. As I expand upon in my analyses in Chapter VII below, there is an extremely high probability that BellTrox is the hack-for-hire company contracted to carry out the cyber-attacks against Mr. Levin and others in connection with the Arbitration Proceeding.

VI. The WY Report

28. The WY Report, referenced above, **highlights the evident success of certain hacking attempts**. Both Mr. Levin and his colleagues received suspicious emails containing links that appeared to originate from Mr. Levin himself, including some from his previously used emails addresses (e.g. Oferlevin@aon.at).¹⁹
29. WY found that these previously used emails of Mr. Levin were hacked and had been traded on the dark web.
30. Additionally, after Mr. Levin provided WY with a potential suspect behind the hacking efforts, Mr. Shamsi, the opposing party to the Arbitration Proceeding, WY employed a counter-tactic in an effort to confirm or disprove Mr. Shamsi's involvement.²⁰

¹⁸ A. Volle, "Dark Web," *Britannica* (December 3, 2024), <https://www.britannica.com/technology/dark-web>; see additional short explanation here: <https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web>.

¹⁹ WYR, pgs.3-5.

²⁰ WYR, pgs.5-6.

31. The strategy was successful, serving as another indicator of Mr. Shamsi's involvement in these hack-for-hire cyber-attacks.²¹
32. While WY's efforts were ongoing, they also received a request for assistance from Mr. Levin's legal counsels from the Levin & Lustigman & Lefer Law Firm ("LLL"), as they had received a communication from Citizen Lab, regarding the handling of evidence collected as part of an arrest and legal proceeding conducted against the Israeli private investigator, Mr. Azari, in the United States.
33. According to the material in Citizen Lab's possession, the services of Mr. Azari were contracted for hacking into LLL's computers. After reviewing the evidence provided by Citizens Lab, WY found that the malware methodology used to hack LLL's computers, was virtually identical to the attack WY had investigated against Mr. Levin.
34. It is important to note that during their investigations, WY also found that Mr. Levin had been impersonated in order to access his government credit pool account in Israel, through Israel's government identification system, allowing the perpetrator to access Mr. Levin's credit reports. An inquiry by WY into the identity of the impersonator failed as the responsible governmental entity responded that it was impossible to know who impersonated Mr. Levin.²²
35. After comparing my investigation to that of WY, it appears that what is characteristic of all the attacks carried out is that they are all targeted at specific email addresses of specific individuals, which indicates that these are not generic attacks that occur regularly in the internet space, but **hack-for-hire targeted attacks**.

VII. My Analysis of the Cyber-Attack Related to the Arbitration Proceeding

36. Based on the information I have been provided with, the cyber-attack in question supposedly constituted a sophisticated and coordinated campaign targeting Mr. Levin and his colleagues, including his legal representatives, LLL, and while there were indications that these attacks were orchestrated by Mr. Shamsi, there was no direct link connecting these hackings to the Arbitration Proceedings.

²¹ Ibid.

²² WYR,pg. 8 .

37. As further detailed below, my investigation found that the attackers employed phishing emails, a widely utilized and effective tactic in such cyber-attacks. These emails were designed to deceive recipients into divulging sensitive information or inadvertently granting access to secure systems. Recipients of such emails were prompted to take specific actions, such as clicking malicious links, downloading malware, or entering personal credentials on counterfeit websites. My in-depth analysis of the specific emails in question can be found in the AIR.²³
38. My analysis of the emails shows that to enhance the effectiveness of their cyber-attacks, the attackers used advanced tracking technologies, such as Readnotify.²⁴ Readnotify is an email tracking tool that provides detailed insights into email interactions. It informs the sender when the recipient opens the email, the recipient's geographical location, the type of device used, and the duration the email was viewed. Additionally, it can reveal whether links within the email were clicked or attachments were opened, further aiding in the precision and adaptability of the phishing strategy.
39. My investigation also uncovered the use of one-pixel tracking images — tiny, invisible images embedded in emails that notify the sender when the email is opened.
40. I compared the information with data we have collected over the years from multiple commercial hackers. As part of this data, we have a large amount of Readnotify logs. Those logs show which emails have been targeted by commercial hackers using the Readnotify tool.
41. The vast majority of phishing emails that were received by LLL were first tested by the hackers on a dummy email that they controlled. The dummy emails in question are thorbackup12@outlook.com and nikitinabackup@outlook.com.

²³ AIR, pgs. 7-15.

²⁴ Readnotify is an enhanced certified email service. It enables reliable tracking of email correspondence, informing the sender when select emails are received and viewed. It also provides certifiable proof that emails are sent, received and viewed by incorporating digital certificate technology and time/date stamping (https://www.readnotify.co/readnotify/about_pm.asp). While Readnotify is a tracking system with legitimate uses, it may also be used by hackers to know if their victims opened their email or not. This tool was in use by the vast majority of commercial hackers until the end of 2017, where most commercial hacking firms started to phase it out and develop their own in-house tools.

42. Commercial hackers regularly send themselves a test email to ensure that their phishing email is credible enough before sending it to their victims. In this instance, before Mr. Levin and LLL were sent a phishing email, the exact same phishing email, with the same title was sent seconds before to those test accounts. They were then sent to multiple victims.²⁵
43. The conclusion from this analysis shows that the IOCs used by the hackers to target Mr. Levin and LLL are the exact same IOCs that have been previously and typically used by BellTrox, these IOCs are usually domain names and URL shortened that are recycled by BellTrox and other hack-for-hire companies for multiple projects. Setting up a hacking infrastructure properly is hard, time consuming and expensive. It is thus normal that said companies recycle domain names and their technological tools for multiple projects. As a result, one can test mailboxes and other IT Infrastructure against known IOCs (or domains/URLs) to see if one has been the recipient of emails originating from hack-for-hire firms and infrastructure.
44. As part of my investigation and in addition to my forensic analysis of the different phishing emails, IOCs and TTPs of BellTrox, I also reached out to multiple sources and contacts in India, with whom I have conducted previous investigations. As part of this effort, I sought to identify employees of BellTrox who might have worked on the project related to the Arbitration Proceeding.
45. I successfully identified [REDACTED]
[REDACTED] Through multiple conversations [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. [REDACTED] affidavit, signed and dated, October 1, 2024 [REDACTED]
[REDACTED], is attached as **Annex 6**.

²⁵AIR, pgs. 3-4.

46. In his affidavit, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

47. He describes [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

48. [REDACTED] explained that '[REDACTED]
[REDACTED]
[REDACTED]

49. He also provided a list of [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

50. This list [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] I was also
informed that [REDACTED]
[REDACTED]

51. The relevant email addresses in the log include:

- offerlevin001@gmail.com
- oren@l-law.co.il
- jonathan@l-law.co.il
- gal@l-law.co.il
- meir@l-law.co.il
- eran@l-law.co.il

- tal@l-law.co.il
- aviz@gglaw.co.il
- avizam@gmail.com
- inbal@santiya.at

52. I note in this regard that the “inbal@santiya.at” email address is one that is specifically discussed in the WY report as the subject of a targeted attack.²⁶

53. I note that the email addresses relating to this Arbitration Proceeding are consistent with hack-for-hire operations as they involve one of the parties, its counsels as well as the arbitrator himself, which negates the possibility that these attacks were random hackings.

54. At my request [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

55. Furthermore, I have confirmed that over 95% of the data on the list above, is included in the data we have gathered over the years. To clarify this, our data has been gathered over the last 4 years from multiple employees and stakeholders of BellTrox. This data is often incomplete and resembles a puzzle of logs, third party data, background data, domains and others which were used by BellTrox to conduct multiple hacking operations around the world. By matching the data obtained by [REDACTED] against the data already in our possession, we note a 95% rate of overlap.

VIII. The Conclusions Arising Out of My Analysis

²⁶WYR, pgs. 6-7.

²⁷[REDACTED] affidavit, pgs. 3-4.

56. As detailed above, I was instructed to carry out my analysis in view of indications that a hacking operation took place against Mr. Levin and his attorneys. This assessment was based on emails they received, the findings outlined in the WY Report, and approaches made by credible third parties, including Reuters and Citizen Lab.
57. An important part of my analysis, is the WY Report, which highlights that, during the timeframe of the Arbitration Proceeding, one of Mr. Levin's email addresses was compromised and subsequently used in phishing attacks, with the associated links traced back to a malicious server. Amongst other things, the WY Report includes a significant indicator of the involvement of Mr. Shamsi or someone on his behalf in the hacking of one of Mr. Levin's emails through the planting of financial information related to subject matter of the Arbitration Proceedings and the underlying economic relationship between Mr. Levin and Mr. Shamsi, which triggered direct action shortly after the relevant email was accessed by the attackers.²⁸
58. First and foremost, my investigation found that not only was Mr. Levin, his legal counsel and his employees targeted, but also the arbitrator in the Arbitration Proceedings – Avi Zamir. This, together with the timing of the attacks, clearly shows that the attack by BellTrox was undoubtedly connected to the Arbitration Proceedings, as there is no other plausible conclusion that would explain the finding of the arbitrator's email addresses (both personal and professional) on the same emails log of Mr. Levin and those related to him.
59. Second, while the information available does not provide direct evidence linking Mr. Shamsi (or anyone acting on his behalf) to the hacking attempts against Mr. Levin, his attorneys, the arbitrator and others involved in the Arbitration Proceedings, partly due to the passage of time, multiple indicators exist evidencing that:
- a. A hack-for-hire operation targeted, among others, Mr. Levin, his attorneys, and the arbitrator involved in the arbitration proceedings.

²⁸WYR, pgs.5-6.

- b. The scope of the attack—evidenced by the number of email addresses targeted, all related to the Arbitration Proceedings—and the absence of evidence indicating attacks on email addresses linked to Mr. Shamsi or his associates strongly suggest that the operation specifically aimed to target Mr. Levin, his affiliates, and the arbitrator.
 - c. Belltrox played a direct role in this commercial hack-for-hire operation, as evidenced by information provided by the IOCs and TTRs, as well as corroborated by [REDACTED] affidavit and logs.
 - d. Mr. Shamsi and his associates have admitted to hiring private investigators in connection with the Arbitration Proceedings.²⁹
 - e. There are substantial indicators linking the involvement of Mr. Shamsi or someone acting on his behalf to the hacking of one of Mr. Levin's email accounts.
 - f. According to WY, there is evidence that someone illegally accessed Mr. Levin's governmental reports, which include credit information and other sensitive personal data.
60. Based on the forensic evidence analyzed above, it can be concluded with a high degree of confidence that the Mr. Levin, his colleagues, and the arbitrator were targeted by Belltrox between 2017 and 2020. Furthermore, considering the nature and scope of these attacks, it is more probable than not that these operations were ordered, directly or indirectly, by Mr. Shamsi.



Signature

20 January 2025

Date

²⁹Plaintiff's Response to the Respondent's Request for orders prohibiting the plaintiffs from contacting various entities, August 18, 2019, para. 14, attached as **Annex 7**.

References:

1. J. Reddick, "American Businessman Settles Hacking Case in UK Against Law Firm," *The Record* (February 5, 2024), <https://therecord.media/american-businessman-settles-hacking-case-against-law-firm-uk>.
2. *Ras Al Khaimah Investment Authority v Azima and Others* [2023] EWHC 2018 (Ch).
3. D. Kirkpatrick, "A Confession Exposes India's Secret Hacking Industry," *New Yorker* (June 1, 2023), <https://www.newyorker.com/news/annals-of-crime/a-confession-exposes-indias-secret-hacking-industry>.
4. R. Satter & C. Bing, "How Mercenary Hackers Sway Litigation Battles," *Reuters* (June 30, 2022), <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>.
5. J. Stubbs, R. Satter & C. Bing, "Exclusive: Obscure Indian Cyber Firm Spied on Politicians, Investors Worldwide," *Reuters* (June 27, 2020), <https://www.reuters.com/article/technology/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUSKBN23G1FI>.
6. D. Ziyaeva & A. Celso Pugliese, "Hacking the System: Admissibility of Evidence from Cyberattacks in Arbitration," *Global Arbitration Review* (July 19, 2024), <https://globalarbitrationreview.com/review/the-arbitration-review-of-the-americas/2025/article/hacking-the-system-admissibility-of-evidence-cyberattacks-in-arbitration>.
7. R. Calvillo Ortiz, "Admissibility of Hacked Emails as Evidence in Arbitration," *Transnational Notes* (May 14, 2018), <https://transnational.law.nyu.edu/2018/05/admissibility-of-hacked-emails-as-evidence-in-arbitration/>.
8. D. Croft, "Clive Palmer-Owned Company Accuses Government of Hacking Its Lawyers During \$300bn Lawsuit," *Cyberdaily* (February 13, 2024), <https://www.cyberdaily.au/security/10175-clive-palmer-owned-company-accuses-government-of-hacking-its-lawyers-during-300b-lawsuit>.
9. A. Ross, "Tribunal Rules on Admissibility of Hacked Kazakh Emails," *Global Arbitration Review* (September 22, 2015), <https://globalarbitrationreview.com/article/tribunal-rules-admissibility-of-hacked-kazakh-emails>.
10. *Dark Basin*, Wikipedia, https://en.wikipedia.org/wiki/Dark_Basin.

11. U.S. Attorney's Office, Northern District of California, **"Private Investigators Indicted in E-Mail Hacking Scheme,"** (February 11, 2015), <https://www.justice.gov/usao-ndca/pr/private-investigators-indicted-e-mail-hacking-scheme>.
12. U.S. Attorney's Office, Southern District of New York, **"Israeli Hacker-for-Hire Sentenced to 80 Months in Prison for Involvement in Massive Spearphishing Campaign,"** (November 16, 2023), <https://www.justice.gov/usao-sdny/pr/israeli-hacker-hire-sentenced-80-months-prison-involvement-massive-spearphishing>.
13. R. Satter, **"Israeli Accused of Hacking Released by UK Authorities Due to Misunderstanding,"** *Reuters* (May 9, 2024), <https://www.reuters.com/world/uk/israeli-accused-hacking-released-by-uk-authorities-due-misunderstanding-2024-05-09/>.
14. J. Uchill, **"Hack-and-Leak for Hire Being Sold as Litigation Assistance,"** *SC Media* (November 16, 2021), <https://www.scworld.com/analysis/hack-and-leak-for-hire-being-sold-as-litigation-assistance>.
15. E. Galperin & C. Quintin, **"Phish for the Future,"** *EFF* (September 27, 2017), <https://www.eff.org/>.
16. C. Rothe, **"'Dark Basin' Hacking Group Targeted Thousands in Hack-for-Hire Scheme,"** *Red Canary*, <https://redcanary.com/company/origin-story/>.
17. A. Volle, **"Dark Web,"** *Britannica* (December 3, 2024), <https://www.britannica.com/technology/dark-web>.

Exhibit 3



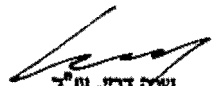
February 9, 2025

CERTIFIED Translation

I, Adv. Sarah Dray, License No. 65176, certify that I am fluent and competent in the Hebrew and English languages, am competent to translate accurately between Hebrew and English and that the attached complete document, entitled

“Expert Opinion - Civil Action 3216-01-25,”

is a true and accurate translation of the original Hebrew file attached.



שרה דריי, עו"ד
65176 רישון
Sarah Dray, Adv
License No. 65176

Expert Opinion

In support of the Motion to Vacate the Arbitration Award (and Answer to the Respondents' Motion to Approve the Arbitration Award, dated January 1, 2025)
In the matter of Civil Action 3216-01-25

Expert's name: Mr. Raphael Balulu.

Address and office: Wizman-Yaar, 7 Metsada Street. B.S.R Tower 4, 39th floor, Bnei-Brak, 5126112, Israel.

I the undersigned, Raphael Balulu, bearer of Israeli ID No. 205379760, a cyber forensic researcher and computer forensic analyst at the Wizman-Yaar business intelligence and investigation company, was requested by the law office of Gornitzky & Co. (hereinafter: "**Gornitzky**"), the legal counsel of the Applicant in the proceedings in question, to file a professional expert opinion on the matter of the cyber-attacks that were conducted against the Applicants, their employees, their clients and other related parties during the arbitration proceeding that is the subject of this Motion. The purpose of the expert opinion is to present the findings of our investigation, which was aimed at identifying the source of the hacking into the computer systems, to determine the scope of the information obtained during the attacks, and to indicate who was responsible for carrying them out.

I am providing this expert opinion report in place of testimony in court, and I hereby declare that I am well aware that with regard to the provisions of criminal law relating to false testimony in court, that this expert opinion report, once it is signed by me, amounts to testimony under oath in court.

The details of my education and professional experience are set forth in Appendix 1 to this expert opinion.

Signed by:

January 25, 2025
Date

[Signature]
Signature

Framework of the Expert Opinion

Over the last decade, cyber-attacks have become more and more common. Since the internet has become a part of daily life, both on a personal and commercial level, general and untargeted cyber-attacks against the public as a whole (the “Nigerian Prince”) have become part and parcel of routine life. Notwithstanding, in recent years we have come to witness more and more dedicated cyber-attacks against pre-selected targets, and these are designed, inter alia, to glean sensitive personal data and commercial information (often without the “target” knowing about it), and to sabotage the proper functioning of computer systems.

These dedicated cyber-attacks are not carried out in a vacuum, and they are usually “ordered” by third parties (hack-for-hire), who seek to attack the targets, and require prior measures to be adopted and meticulous preparation for them to be implemented. Based on our experience in this field, in the large majority of cases in which a “target” is selected for a cyber-attack, the hackers will precede their attack by engaging in prior intelligence collection on the dark net regarding the target’s internet history, and will attempt to locate email addresses belonging to the target that have already been hacked, the “target’s” passwords that are on sale to the highest bidder, as well as other weaknesses in their security system.

These dedicated attacks are different in their nature and characteristics from general attacks, and in light of the replacement of devices, security updates and monitoring of the networks under attack, they usually last for a long period of time, in an attempt to grant direct and continuous access to the “target’s” computers and the data stored in them.

In our case, we were asked to examine, in light of various indications as to the existence of cyber-attacks against Levin, his employees, attorneys and other entities, whether these were indeed dedicated attacks launched against Levin and/or those entities related to him and whether it was possible to identify various entities who might be behind those attacks.

Subsequent to the examination of the evidence provided for our review and following various investigative actions that we engaged in, we identified that dedicated cyber-attacks were indeed carried out against Levin, his employees, and apparently also his attorneys. During the process of gathering the information, data and details emerged that reinforced Levin’s assessment, which was that the person behind this offensive was Mr. Edmund Shamsi.

Documents and data

In order to prepare this expert opinion, we made use of the following documents:

1. Email messages suspected of being phishing emails.
2. An expert opinion of Mr. Jonas Rey.
3. The correspondence of Citizen Lab with Levin’s attorney’s office.
4. Log files.
5. Additional documents that we located on the internet relating to the private investigator Aviram Azari.

In addition to the documents that we reviewed, we also held a number of background conversations with Mr. Levin and attorneys from the law office of Gornitzky & Co., which helped us in preparing this expert opinion, and the information and data provided to us in them are set forth as part of this expert opinion.

Expert Opinion Chapters

1. Chapter 1 – The Case.....	3
2. Chapter 2 – The Activity and its Findings.....	3
3. Chapter 3 – Conclusion.....	10

Chapter 1 – The Case

1. This expert opinion is submitted as an in-depth summary of a whole range of findings that were obtained from the investigative activity carried out subsequent to significant “phishing” attacks carried out against Mr. Ofer Levin (hereinafter: “**Levin**”) and a number of companies related to him.
2. The expert opinion provides a chronological sequence of events, as they were brought to our attention, together with the investigative activities we carried out and the findings gathered.

Chapter 2 – The Activity and its Findings

3. According to the material information provided to us by Levin, on July 22, 2019, Mr. David Fradis (hereinafter: “**Fradis**”), a client of GTI, alerted the company managers to the fact that a suspicious email had been received that contained a link disguised as a message from Levin.
4. Fradis became suspicious in light of two extremely suspicious indicators: firstly, the mail was written in German – a language that Levin had never corresponded in, and secondly, an extremely unusual recipient list was identified.
5. Subsequent to these suspicious findings, an urgent request was sent to our office to conduct a comprehensive forensic check of the email.
6. In the initial investigation that we conducted with Levin, he made it absolutely clear that he had not sent the message in question.
7. Moreover, Levin revealed a critical detail to us: the email address appearing in the signature of the message is a former email address that he used around 2010, and since then he has ceased to use it.
8. This address was provided to him by the Austrian internet service provider Aon, and the email address is: Oferlevin@aon.at, (hereinafter: “**Aon**”).
9. Levin noted, significantly, that the majority of recipients on this message are historical contacts with whom he had been in contact in the past.
10. This list constitutes the original contacts database that belongs to the old email address during the period of use of the said email address, which, as previously stated, has not been active for many years.
11. It is noteworthy that Levin himself is included among the list of addressees, with his other email address (oferlevin001@gmail.com).
12. The malicious messages are attached below:

From: oferlevin <geejolive@techsupportalert.com>
 Date: Mon, Jul 22, 2019 at 8:50 PM
 Subject: Re:Grüß dich, wie geht es dir?
 To: Ofer Levin <oferlevin001@gmail.com>, Naftali Tooly Ungar <deartooly@gmail.com>, david goldberg <d123453@gmail.com>, david fradis <davidfradis@gmail.com>, hai bahalul <haibahalul@gmail.com>

Ich glaube es kaum! www.ruscodisic1980.blogspot.cl

Mach's gut
 oferlevin@aon.at

13. In the comprehensive check that we conducted of the link attached to the suspicious mail, a finding of concern emerged: the link was identified and labeled as clearly malicious on a number of security systems and leading link scanning services.

The screenshot shows a URL scanning interface. At the top, a red circle with the number '2' indicates that 2 engines detected the URL. Below this, the URL 'http://ruscodisic1980.blogspot.cl/' is displayed, along with its status (200), content type (text/html; charset=UTF-8), and timestamp (2020-06-27 06:00:42 UTC). A table below shows detection results from various engines:

DETECTION	DETAILS	COMMUNITY
CyRadat	Malicious	Fortinet
Forcepoint ThreatSeeker	Suspicious	ADMINUSLabs
		Clean
		Clean

14. Following the discovery that the malicious mail was sent as part of a focused attack to a unique address list appearing in the contacts directory of the email in question (Aon), we conducted an in-depth investigation to locate the source of the leak.
15. By using the HIBP service that specializes in locating accounts that have been hacked, a finding of special concern was exposed: said email address (Aon) was identified as a hacked account traded on the dark web – as part of a list of email addresses termed Mail_Access_By_Daniel.
16. The following is a visual documentation of the list (Mail Access By Daniel), which corroborates the fact that Levin's email address is indeed located in the hacked database:

```

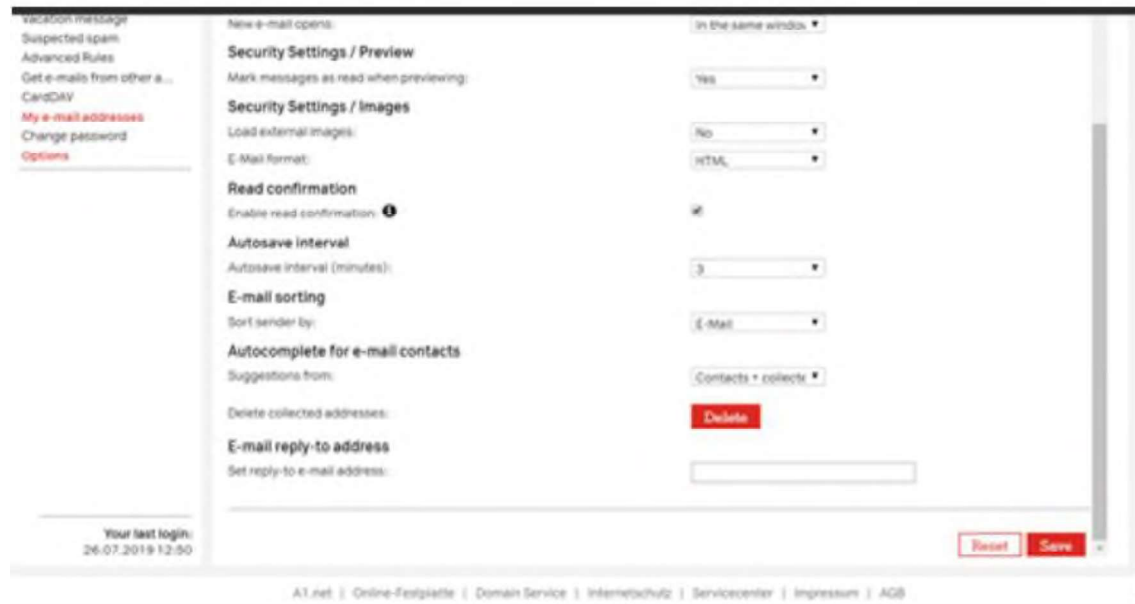
IVAN.DEFALCO@cheapnet.it:300786
sk@arcor.de:kaffee
naturgeil666@t-online.de:Pofotze668
erickrb@numericable.fr:mairie
katekiro@katamail.com:luporosso
kurii@arcor.de:telimail
rico.piller@arcor.de:bubusch
dumbol23-91@gg2.pl:dgqxu9hc
marciniak.monika@poczta.fm:klasyfikacja
v.horeglad@arcor.de:paula2008
ernst.edenharter@arcor.de:Ecotango
beaterenzi@t-online.de:Schicht02
oferlevin@aon.at:1313olol
flavien.scherdel@noos.fr:nounours
alfredo.cognati@cheapnet.it:Alfredo
katariinajee07@hotmail.com:Kertu1234
andy_friedrich86@t-online.de:62403581Andy
arminloevenich@t-online.de:Wotan100
philipp.kirchner@arcor.de:pk200587
advantage81@cheapnet.it:carlatiano
aon.husak@aon.at:cghadzei1999
stonly@ziggo.nl:kizmo0
afpi69@numericable.fr:424242
tam.gold@arcor.de:jason2209
nicgr@cheapnet.it:nicgr500

```

17. After we received access to the mailbox, an additional worrying picture of the situation was exposed: we identified numerous unauthorized entries to the mailbox even after Levin had ceased to use it. The inevitable conclusion was that the attacks had been carried out by someone who had gained unauthorized access to the mailbox.
18. Later on, during the investigation, we initiated a sophisticated move to identify who had gained unauthorized access to this mailbox, apart from the access that was given to the investigation team by Levin.
19. A critical point emerged during the in-depth questioning of Levin, when he pointed to a potential suspect who might be behind the hacking of the mailbox and sending of the malicious link – Mr. Edmund Shamsi (hereinafter: “**Shamsi**”), with whom he has been in an ongoing legal dispute for some time.
20. In order to verify or refute Levin’s suspicion as to Shamsi’s involvement, we planned and implemented an additional investigative step.
21. This included the strategic planting of a fictitious message in the Aon email box.
22. The content of the message was meticulously planned and included an apparent authorization from the Austrian Bawag PSK bank for the withdrawal of a considerable sum of half a million dollars from Levin’s bank account and the transfer of that sum to the bank account of a company called PARDESS in Brazil.
23. It should be pointed out in this context, according to the information that Levin provided us, PARDESS was a key point of contention in the ongoing dispute at that time between Levin and Shamsi.
24. Below is the precise message that we planted in the mailbox:



25. In a direct follow-on to the investigative act, entry into the Aon mailbox was documented after the date on which the fictitious message was planted.



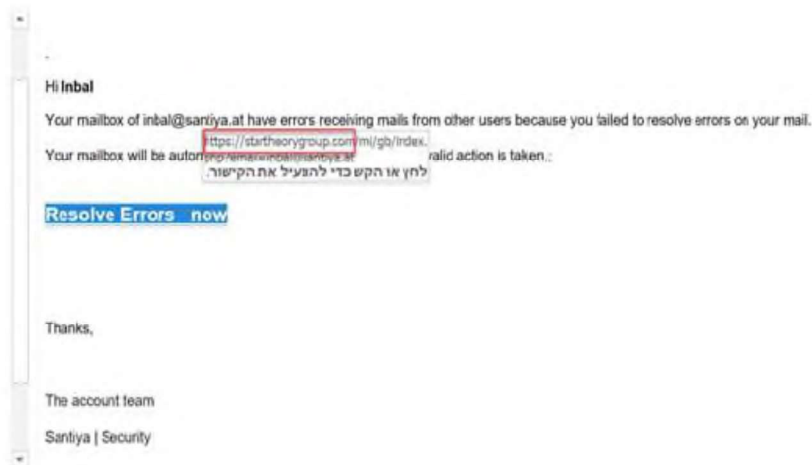
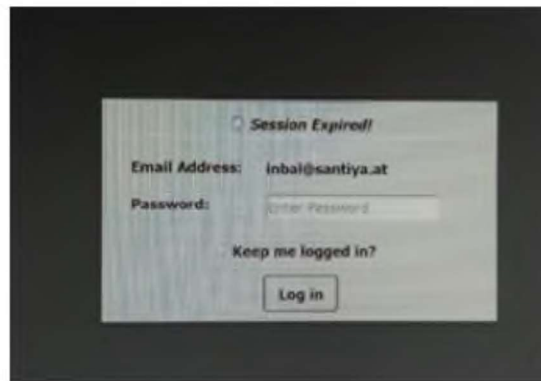
26. Levin provided us with a crucial discovery: subsequent to the planting of the message, Shamsi's accountant, CPA Eran Benita, in a highly unusual step, made contact with Mr. Yehoshua (Joshua) Dalven, the business manager of PARDESS in Brazil, with a request to look at the financial state of the company.
27. This development significantly bolstered Levin's suspicion that the information planted in the mailbox had come into Shamsi's possession, which led to his accountant's inquiry. It is important to point out that Levin stressed to us that prior to this inquiry, there had been no communication between CPA Eran Benita and Mr. Levin for an extremely long time.
28. Pursuant to the information that Levin provided us, following the initial malicious message (that was identified in July 2019) Levin continued to receive suspicious emails.
29. Analysis of the emails showed that their characteristics might be consistent with the activity of paid, professional hacking services.

30. To date, a number of messages have been documented that **successfully penetrated the advanced security mechanisms** of both the private and the business email boxes.
31. Below are a number of examples of phishing messages that succeeded in penetrating the security mechanisms:
- Example of a message sent to an employee, Noga Mann-Gruber

This employee made use of a mailbox belonging to a former employee in the company by the name of Inbal.

In this sophisticated attack, a link disguised as an original password reset screen was sent, with the entire content of the message serving as the link.

Below is a picture of the fictitious “password reset” screen:



32. Below is an example of a message containing a malicious link that was sent to the GTI mailbox to two clients of the fund and to Levin himself, supposedly from Mr. Levin:



33. At the same time, our office (Wizman-Yaar Intelligence and Investigations) received a request from the law firm of Lustigman, Lefler & Co.
34. This is a law office that provides legal services, inter alia, to Levin, and as Levin told us, Adv. Oren Lustigman was a witness in the arbitration proceeding conducted between Levin and Shamsi.
35. The people who spoke with us stated that they received a request from Canadian group, Citizen Lab. This is an academic research institute from the University of Toronto that deals with computer sciences.
36. Citizen Lab informed the attorneys, (Lustigman, Lefler) that they had been entrusted with dealing with the evidentiary material collected as part of the arrest and legal proceedings being conducted against the Israeli private investigator Aviram Azari, in the US.
37. This relates to an incident in which the private investigator Aviram Azari (who at the time was himself operating in the US), was suspected of supplying computer hacking services in consideration for substantial amounts of money.
38. It should be emphasized that the attorneys believed that the purpose of the attempts to hack into the firm's computers, insofar as this was done, was to collect sensitive information relating to their client, Levin.
39. Moreover, from a review of the materials handed over to us, including the indictment against Aviram Azari, it emerges that the cyber-attack methodology described in it shares identical characteristics to the attack that we investigated and found to be aimed at Mr. Levin.

victims, located in the Southern District of New York and elsewhere, by sending false and fraudulent emails to those victims, in order to trick the victims into entering their usernames and passwords to their electronic accounts into false and fraudulent websites controlled by AZARI and his co-

40. An additional significant and noteworthy incident is the impersonation of Mr. Levin and hacking in his name into Israel's government Credit Data Register. It should be noted that in Israel, it is possible to obtain a credit rating report via a multi-stage identification process in the government identification system. In August 2019, Levin applied to be registered in the government identification system only to discover that another person had already registered in his name while falsifying details (credit card and ID or passport numbers). An inquiry conducted with the

Supervisor of Credit Data Sharing revealed that it was not possible to know who had impersonated Levin.

41. As set forth in Mr. Jonas Rey's expert opinion, which is filed together with this expert opinion of ours, during the initial years of the arbitration proceeding, the hacking attacks into Levin's computers and entities associated with him, were carried out via BellTrox, which ceased to operate in 2021 (inter alia, subsequent to the filing of the indictment against Aviram Azari).
42. However, in checks carried out after 2021, a number of additional hacking attempts targeting Mr. Levin were identified.
43. Below is an example of a message sent in 2023 to Levin's mailbox, and that of an individual named Nadav Rotemberg-Shir, who we were told is a former client of GTI. This message contains a link identified as a malicious link by Phishfort.



44. In addition to the aforementioned, on February 14, 2022, in the period immediately subsequent to the cessation of BellTrox's activity, Levin reported to us a case of unusual behavior of his iPhone, which took the form of repeated crashes, the 'freezing' of a number of apps, and the unusual activation of the phone's microphone notification without him having initiated this.
45. Our examination of Levin's telephone revealed that the apps that had been affected were Google, Safari, Apple Store, Chrome and Mozilla Firefox. Below is a crash log of the Safari app on Mr. Levin's phone, which is indicative of unusual activity, and which is consistent with the existence of the hacking of the phone's security.


```

\fs24 \cf0 Incident Identifier: 45678901-12KL-6789-MNOP-2345678901CD\
CrashReporter Key: cdef1234567890abcdef1234567890abcdef56\
Hardware Model: iPhone14,3\
OS Version: iOS 15.3 (19D50)\
Kernel Version: Darwin Kernel Version 21.3.0\
Date: 2022-02-14 10:32:15 +0000\
Time Since Boot: 3900 seconds\
\
Application: Safari\
Identifier: com.apple.mobilesafari\
Version: 604.1.34\
Process: Safari [2345]\
Path: /Applications/Safari.app/Safari\
Parent: launchd [1]\
Exception Type: EXC_BAD_ACCESS (SIGSEGV)\
Exception Subtype: KERN_INVALID_ADDRESS at 0x000000000000020\
Exception Codes: 0x0000000000000001, 0x000000000000020\
VM Regions Near 0x20:\
--> \
__TEXT 0000000100000000-0000000101000000 [ 16.0M] r-x/r-x SM=COW /Applications/Safari.app/Safari\
\
Triggered by Thread: 7\

```

46. All the aforementioned apps are affected by WebKit (an open code browser engine that mainly serves Apple's operating system).
47. In reply to our question, Levin stated that the unusual behavior commenced immediately after opening email messages from an unidentified sender containing a PDF file.
48. This behavior corresponds with a serious security breach termed CVE-2022-22620, which was exposed on February 11, 2022, only three days prior to this. This breach exposed devices and browsers that had not been updated to significant damage.
49. From our experience, the immediate use of vulnerabilities of this type, especially immediately after they have been publicized, is a common practice in focused attack attempts.
50. Following our instructions, Levin carried out an immediate security update, and subsequently, all the unusual forms of behavior immediately disappeared.
51. This bolstered the assessment that Levin's mobile phone had been hacked using the said vulnerability.

Chapter 3 – Conclusion

52. The information set forth above speaks for itself.
53. Analysis of all the data, as brought in the body of this report, paints a clear picture of focused and precision attacks, which were directed at specific email addresses subsequent to prior intelligence collection. These attacks are not generic or routine attacks, but rather the result of paid and planned actions, clearly targeting Levin, his employees, clients and attorneys.
54. These attempted attacks against Levin continued for several years and were carried out both using BellTrox (as set forth in Rey's expert opinion), and in the subsequent years as well, after BellTrox ceased operating.
55. During the gathering of the information, data and details emerged supporting Levin's assessments, according to which the figure behind this offensive was Shamsi.

Yours sincerely,

[Signature]

Wizman-Yaar

חוות דעת מומחה

לתמיכה בבקשה לביטול פסק הבוררות (ותשובה לבקשת המשיבים מיום 1.1.2025 לאישור פסק הבוררות)

בעניין ת"א 3216-01-25

שם המומחה : מר רפאל בלולו.

מען ומשרד : ויצמן יער, מצדה 7, מגדלי בשר 4, קומה 39, בני ברק, 5126112, ישראל.

אני הח"מ, רפאל בלולו ת.ז. 205379760, חוקר סייבר וראיות מחשב בחברת ויצמן יער מודיעין עסקי וחקירות, התבקשתי על ידי משרד עו"ד גורניצקי ושות' (להלן: "גורניצקי"), ב"כ המבקשת בהליך דנן, להגיש חוות דעת מקצועית בעניין מתקפות הסייבר שבוצעו כנגד המבקשים, עובדיהם, לקוחותיהם וצדדים קשורים אחרים במהלך הליך הבוררות נשוא בקשה זו. מטרת חוות הדעת הינה להציג את ממצאי חקירתנו שמטרתה לזהות את מקור החדירות למערכות המחשוב, לאפיין את היקף המידע שהושג במסגרתן, ולהצביע על הגורם האחראי לביצוען.

אני נותן חוות דעתי זו, במקום עדות בבית המשפט ואני מצהיר בזאת כי ידוע לי היטב, שלעניין הוראות החוק הפלילי בדבר עדות שקר בשבועה בבית המשפט, דין חוות דעת זו כשהיא חתומה על ידי, כדין עדות בשבועה שנתתי בבית המשפט.

פרטי השכלתי וניסיוני המקצועי מפורטים **בנספח 1** לחוות דעת זו.

על החתום :



25.01.25

חתימה

תאריך

מסגרת חוות הדעת

בעשור האחרון הפכו מתקפות סייבר נפוצות יותר ויותר. מאז נכנס האינטרנט לחיי היום-יום, האישיים והמסחריים, הפכו מתקפות סייבר כלליות ובלתי ממוקדות כנגד הציבור בכללותו ("הנסיך הניגרי") לדבר שבשגרה. עם זאת, בשנים האחרונות מזוהות יותר ויותר מתקפות סייבר ייעודיות שמטרתן נבחרת מראש, והן נועדו, בין היתר, לדלות מידע אישי ומסחרי רגיש (לעתים ללא ידיעת ה"יעד"), ולחבל בפעילות התקינה של מערכות מחשב.

תקיפות סייבר ייעודיות אלה אינן מתבצעות בחלל ריק, והן בדרך כלל "מוזמנות" על ידי צדדים שלישיים (Hack for Hire), המעוניינים בתקיפת היעדים, ומחייבות היערכות מקדימה והכנה מדוקדקת לצורך ביצוע. מניסיונו בתחום, ברובם המכריע של המקרים בהם נבחר "יעד" לתקיפת סייבר, יבצעו ההאקרים התוקפים איסוף של מודיעין מקדים ב"רשת האפילה" (Dark Net) אודות היסטוריית השימוש של היעד באינטרנט וינסו לאתר כתובות דוא"ל של היעד שכבר נפרצו, סיסמאות של ה"יעד" שמוצעות למכירה בתשלום למרבה במחיר, וחולשות במערכת האבטחה שלו.

תקיפות ייעודיות אלה שונות באופיין ובמאפיינים שלהן מתקיפות כלליות, ולאור החלפות מכשירים, עדכוני אבטחה, וניטור של הרשתות המותקפות, הן לרוב נמשכות תקופה ארוכה, בניסיון להעניק גישה ישירה ומתמשכת למחשבי ה"יעד" ולמידע האגור בתוכם.

בענייננו, התבקשנו לבחון, לאור אינדיקציות שונות לקיומן של תקיפות סייבר כנגד לוי, עובדיו, עורכי דינו וגורמים אחרים, האם אכן בוצעו תקיפות ייעודיות כנגד לוי ו/או גורמים הקשורים לו, והאם ניתן לזהות גורמים שונים, אשר ייתכן שעומדים מאחורי אותן תקיפות.

לאחר בחינת הראיות שהועברו לעיונו, ובעקבות פעולות חקירה שונות שביצענו, זיהינו כי אכן בוצעו תקיפות סייבר ייעודיות כנגד לוי, עובדיו, וכפי הנראה גם עורכי דינו. במהלך איסוף המידע, עלו נתונים ופרטים אשר חיזקו את הערכותינו של לוי ולפיהן מי שעומד מאחורי המתקפה הינו מר אדמונד שמסי.

מסמכים ונתונים

לצורך הכנת חוות דעת זו עשינו שימוש במסמכים הבאים:

1. הודעות דוא"ל שנחשדו כדואר דיג (פשינג).
2. חוות דעת מומחה של מר Jonas Rey.
3. פניית Citizen Lab אל משרד עורכי הדין של לוי.
4. קבצי לוג
5. מסמכים נוספים שאיתרנו ברשת האינטרנט הנוגעים לחוקר הפרטים אבירם עזרי.

בנוסף למסמכים בהם עיינו, קיימנו גם מספר שיחות רקע עם מר לוי ועם עורכי הדין ממשרד גורניצקי ושות', אשר סייעו לנו בהכנת חוות הדעת, ואשר המידע והנתונים שנמסרו לנו במסגרתם מפורטים במסגרת חוות דעת זו.

פרקי חוות הדעת

1. פרק א' – המקרה..... 3
2. פרק ב' – הפעילות וממצאיה..... 3
3. פרק ג' – סיכום..... 10

פרק א' - המקרה

1. חוות דעת זו מוגשת כסיכום מעמיק של מכלול הממצאים שהתקבלו מהפעילות החקירתית שבוצעה בעקבות מתקפות "פשינג" משמעותיות שבוצעה כנגד מר עופר לוי (להלן: "לוי") ומספר חברות המקושרות אליו.
2. במסגרת חוות הדעת יפורט באופן כרונולוגי רצף השתלשלות האירועים, כפי שהובא לידיעתנו, תוך פירוט פעולות החקירה שביצענו והממצאים שנאספו.

פרק ב' – הפעילות וממצאיה

3. על פי המידע המהותי שהועבר אלינו על ידי לוי, בתאריך: 22 יולי 2019, התריע מר דוד פרדיס (להלן: "פרדיס"), לקוח של חברת GTI, בפני מנהלי החברה על קבלת מייל חשוד הכולל קישור המתחזה למייל מלוי.
4. חשדו של פרדיס התעורר לנוכח שני סממנים מחשידים מובהקים: ראשית, המייל נוסח בשפה הגרמנית - שפה בה לוי מעולם לא התכתב עמו, ושנית, זוהתה רשימת נמענים חריגה בתכלית.
5. בעקבות הממצאים המחשידים, הועברה פנייה דחופה למשרדנו לביצוע בדיקה פורנזית מקיפה של המייל.
6. בחקירה הראשונית שערכנו מול לוי, הוא הבהיר באופן נחרץ כי לא שלח את ההודעה המדוברת.
7. יתרה מזאת, לוי חשף בפנינו פרט קריטי: כתובת המייל המופיעה בחתימת ההודעה הינה כתובת היסטורית שהייתה בשימוש בסביבות שנת 2010, וזנח אותה מאז.
8. כתובת זו סופקה לו על ידי ספק אינטרנט האוסטרי Aon, כתובת המייל היא: Oferlevin@aon.at, (להלן: "Aon").
9. באופן משמעותי, ציין לוי, כי מרבית הנמענים להודעה הינם אנשי קשר היסטוריים, עמם היה בקשר בעבר.
10. רשימה זו מהווה את מאגר אנשי הקשר המקורי המשוך בתקופת השימוש בכתובת המייל הנדונה לכתובת המייל הישנה, אשר כאמור אינה פעילה מזה שנים.
11. ראוי לציון כי בין הנמענים נכלל גם לוי עצמו, בכתובת מייל אחרת שלו (oferlevin001@gmail.com).
12. מצ"ב ההודעה הזדונית:

- 4 -

From: oferlevin <geejolive@techsupportalert.com>
 Date: Mon, Jul 22, 2019 at 8:50 PM
 Subject: Re:Grüß dich, wie geht es dir?
 To: Ofer Levin <oferlevin001@gmail.com>, Natfali Tooly Ungar <deartooly@gmail.com>, david goldberg <d123453@gmail.com>, david fradis <davidfradis@gmail.com>, hai bahakul <haibahakul@gmail.com>

Ich glaube es kaum! www.ruscodisic1980.blogspot.cl

Mach's gut
 oferlevin@aon.at

13. בבדיקה המקיפה שביצענו על הקישור שצורף למייל החשוד, התגלה ממצא מדאיג: הקישור זוהה וסומן כזדוני באופן ברור במספר מערכות אבטחה ושירותי סריקת קישורים מובילים.

The screenshot shows a security tool interface with a top bar indicating '2 engines detected this URL'. Below this, the URL 'http://ruscodisic1980.blogspot.cl/' is displayed along with its status (200), content type (text/html; charset=UTF-8), and a timestamp (2020-06-27 08:00:42 UTC). A 'Community Score' of 2/75 is shown on the left. The main section is divided into three tabs: DETECTION, DETAILS, and COMMUNITY. Under the DETECTION tab, two engines are listed: CyRadar, which flagged the URL as 'Malicious', and Fortinet, which flagged it as 'Phishing'. Below these, Forcepoint ThreatSeeker is listed with a 'Suspicious' flag. At the bottom, there are 'Clean' buttons for ADMINUSLabs and another 'Clean' button with a green checkmark.

14. בעקבות הגילוי כי המייל הזדוני נשלח באופן ממוקד לרשימת כתובות ייחודית המופיעה בספר אנשי הקשר של כתובת המייל הנדונה (Aon), ערכנו חקירה מעמיקה לאיתור מקור הדליפה.

15. באמצעות שימוש בשירות HIBP המתמחה באיתור חשבונות שנפרצו, נחשף ממצא מטריד במיוחד: כתובת המייל המדוברת (Aon) אותרה כחשבון פרוץ הנסחר ב DARKWEB - כחלק מרשימת חשבונות מיילים המכונה Mail_Access_By_Daniel.

16. להלן תיעוד חזותי של הרשימה (Mail Access By Daniel), המאשר את הימצאות כתובת המייל של לויין במאגר הפרוץ:

- 5 -

```

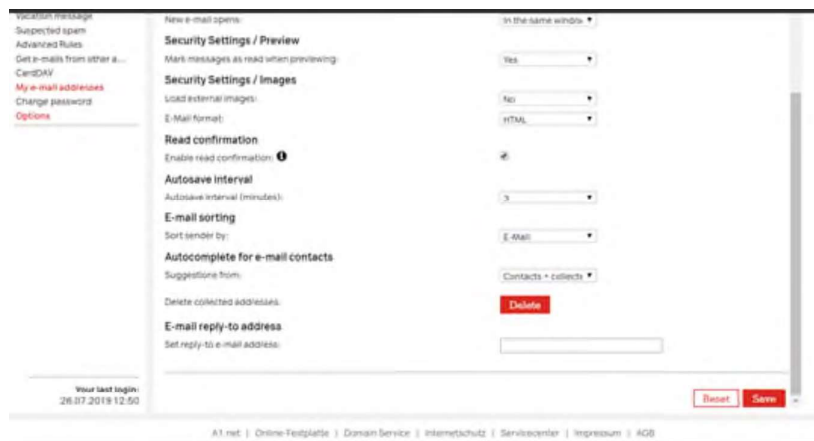
IVAN.DEFALCO@cheapnet.it:300786
sk@arcor.de:kaffee
natureil666@t-online.de:Pofotze668
erickrb@numericable.fr:mairie
katekiro@katamail.com:luporosso
kurii@arcor.de:telima11
rico.piller@arcor.de:bubusch
dumbo123-91@go2.pl:dgqxu9hc
marciniak.monika@poczta.fm:klasyfikacja
v.horeglad@arcor.de:paula2008
ernst.edenharter@arcor.de:Ecotango
beaterenzi@t-online.de:Schicht02
oferlevin@aon.at:1313olol
flavien.scherdel@noos.fr:nounours
alfredo.cognati@cheapnet.it:Alfredo
katariinajee07@hotmail.com:Kertu1234
andy_friedrich86@t-online.de:62403581Andy
arminloevenich@t-online.de:Wotan100
philipp.kirchner@arcor.de:pk200587
advantage81@cheapnet.it:carlatiamo
aon.husak@aon.at:cqhadzei1999
stonly@ziggo.nl:kizmoo
afpi69@numericable.fr:424242
tam.gold@arcor.de:jason2209
nicgr@cheapnet.it:nicgr500

```

17. לאחר שקיבלנו גישה לתיבת המייל, נחשפה תמונה מטרידה נוספת: התגלו כניסות מרובות ובלתי מורשות לתיבה גם לאחר שליון חדל להשתמש בה. המסקנה המתבקשת הייתה כי התקיפות בוצעו על ידי גורם שהשיג גישה בלתי מורשית לתיבה.
18. בהמשך החקירה, יזמנו מהלך מתוחכם במטרה לזהות את הגורם אשר לו היתה גישה בלתי מורשית לתיבה זו, מלבד הגישה שניתנה לצוות החקירה על ידי ליון.
19. נקודה קריטית עלתה במהלך תחקור מעמיק של ליון, כאשר הצביע על חשוד פוטנציאלי שעשוי לעמוד מאחורי הפריצה לתיבת המייל ושליחת הקישור הזדוני – מר אדמונד שמסי (להלן: "שמסי"), המצוי עמו בסכסוך משפטי מתמשך.
20. לצורך אימות או שלילת החשד של ליון באשר למעורבותו של שמסי, תכננו וביצענו מהלך חקירתי נוסף.
21. המהלך כלל השתלה אסטרטגית של הודעה פיקטיבית בתיבת הדוא"ל Aon.
22. תוכן ההודעה תוכנן בקפידה וכלל אישור כביכול מהבנק האוסטרי Bawag PSK למשיכה משמעותית בסך חצי מיליון דולר מחשבון הבנק של ליון והעברתו לחשבון בנק של חברת PARDESS בברזיל.
23. יש לציין בהקשר זה כי בהתאם למידע שמסר לנו ליון, חברת PARDESS היוותה נקודת מחלוקת מרכזית בסכסוך שהתנהל באותה התקופה בין ליון לשמסי.
24. להלן ההודעה המדויקת ששלחנו בתיבת המייל:



25. בהמשך ישיר למהלך החקירתי, תועדה כניסה לחשבון הדוא"ל Aon לאחר מועד השתלת ההודעה הפיקטיבית.



26. גילוי מכריע נמסר לנו מלוי: בעקבות השתלת ההודעה, רו"ח של שמסי, רו"ח ערן בניטה, יצר קשר באופן בלתי שגרתי עם מר יהושע דלויין, המנהל העסקי של חברת PARDESS בברזיל, בבקשה לבירור מצב הכספים בחברה.

27. התפתחות זו חיזקה משמעותית את החשד של לויין כי המידע המושתל בתיבת הדואר הגיע לידינו של שמסי, מה שהוביל לפניית רואה החשבון שלו. חשוב לציין כי לויין הדגיש בפנינו שקודם לפנייה זו היה נתק ממושך בין רו"ח ערן בניטה לבין מר לויין.

28. בהתאם למידע שמסר לנו לויין, מאז ההודעה הזדונית הראשונית (שאותרה ביולי 2019) לויין המשיך לקבל מיילים חשודים.

29. ניתוח של המיילים העלה כי מאפייני המיילים עשויים להיות תואמים לפעילות של שירותי פריצה מקצועיים בתשלום.

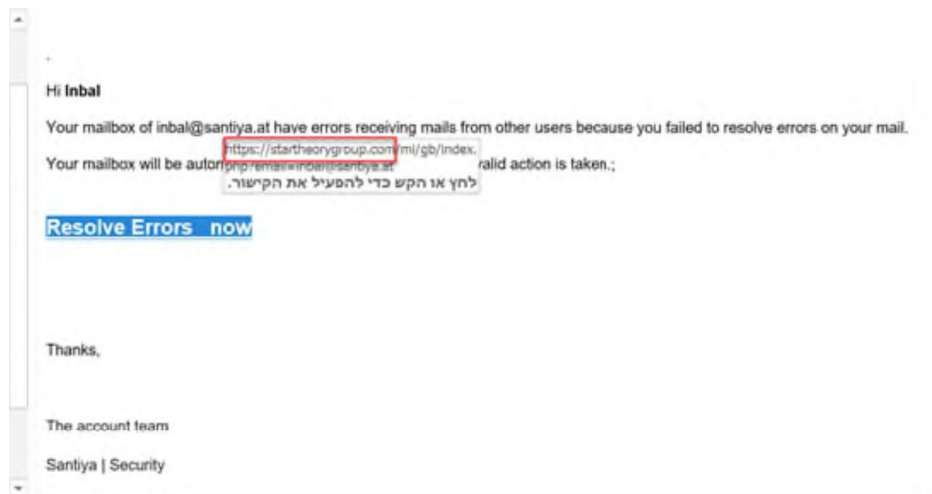
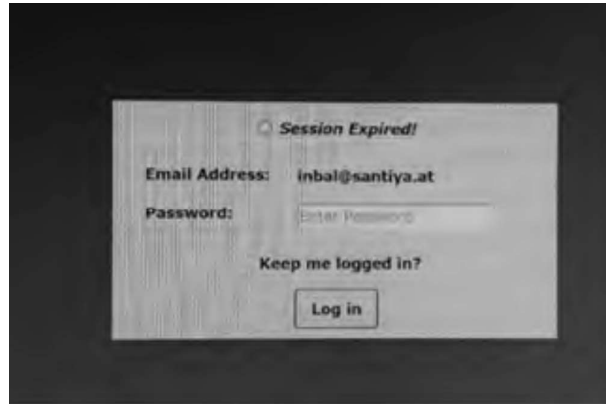
30. עד כה תועדו מספר הודעות שהצליחו לחדור את מנגנוני האבטחה המתקדמים של תיבות המייל הפרטיות והעסקיות.

31. להלן מספר דוגמאות להודעות Phishing שהצליחו לחדור את מנגנוני האבטחה:

- דוגמא של הודעה שנשלחה לעובדת נוגה מן – גרובר

- 7 -

עובדת זו, עשתה שימוש בתיבת דואר של עובדת לשעבר בחברה, בשם ענבל.
 במתקפה מתוחכמת זו, נשלח קישור שהתחזה למסך איפוס סיסמה מקורי, כאשר כל תוכן ההודעה
 שימש כקישור.
 להלן תיעוד מסך "איפוס הסיסמה" הפיקטיבי:



32. דוגמא להודעה המכילה קישור זדוני שנשלחה לתיבת המייל של חברת GTI, לשני לקוחות של הקרן וללויין עצמו, לכאורה ממר לויין:



33. במקביל, התקבלה פנייה למשרדנו (ויצמן יער מודיעין עסקי וחקירות) מפירמת עורכי הדין לוסטיגמן, לפלר.

34. מדובר במשרד המעניק בין היתר, שירותים משפטיים לליון, וכפי שנמסר לנו ע"י ליון, עו"ד אורן לוסיטיגמן, היה עד בהליך הבוררות שהתנהל בין ליון לבין שמסי.
35. בני שיחנו ציינו כי הם קיבלו פנייה מקבוצת CITIZEN LAB, הקנדית. מדובר במכון מחקר אקדמי מאוניברסיטת טורונטו, שעוסק בתחום מדעי המחשב.
36. CITIZEN LAB, עדכנו את עורכי הדין (לוסיטיגמן, לפלר), כי הם קבלו לידיהם את הטיפול בחומר הראיות שנאסף במסגרת מעצרו וההליך המשפטי שמתנהל נגד החוקר הפרטי הישראלי, אבירם עזרי, בארה"ב.
37. מדובר באירוע בו החוקר הפרטי אבירם עזרי (שפעל באותה תקופה בארה"ב עצמה), נחשד במתן שירותי פריצה למחשבים בתמורה לסכומי כסף משמעותיים.
38. יש להדגיש כי עורכי הדין העריכו שמטרת ניסיונות הפריצה למחשבי הפירמה, ככל שנעשו, הייתה איסוף מידע רגיש הנוגע ללקוחם, ליון.
39. נוסף על כך, מעיון בחומרים שהועברו אלינו, כולל כתב האישום נגד אבירם עזרי, עולה כי מתודולוגיית התקיפה המתוארת בו בעלת מאפיינים זהים לזו שנחקרה על ידנו ונמצאה מכוונת כלפי מר ליון.

victims, located in the Southern District of New York and elsewhere, by sending false and fraudulent emails to those victims, in order to trick the victims into entering their usernames and passwords to their electronic accounts into false and fraudulent websites controlled by AZARI and his co-

40. אירוע משמעותי נוסף הראוי לציון הינו התחזות ופריצה בשמו של ליון למאגר האשראי הממשלתי בישראל. יש לציין כי בישראל, ניתן לקבל דו"ח דירוג אשראי באמצעות הזדהות רב-שלבית במערכת ההזדהות הממשלתית. באוגוסט 2019 פנה ליון להירשם למערכת ההזדהות הממשלתית וגילה כי אדם שאינו הוא נרשם על שמו תוך זיוף פרטים (מספרי כרטיס אשראי ותעודת זהות או דרכון). בירור שנערך מול הממונה על שיתוף נתוני אשראי העלה כי לא ניתן לדעת מי התחזה לליון.
41. כמפורט בחוות דעתו של מר Jonas Rey, המוגשת יחד עם חוות דעתנו זו, בשנים הראשונות להליכי הבוררות, הפריצות שבוצעו למחשבי ליון וגורמים הקשורים אליו, בוצעו באמצעות חברת Belltrox. אשר הפסיקה את פעילותה בשנת 2021 (בין היתר, לאחר הגשת כתב האישום נגד אבירם עזרי).
42. עם זאת, בבדיקות שביצענו לאחר שנת 2021, זוהו מספר ניסיונות פריצה נוספים למר ליון.
43. דוגמא להודעה שנשלחה בשנת 2023 לתיבת המייל של ליון, ושל אדם בשם נדב רוטמברג שיר אשר נמסר לנו כי הוא לקוח לשעבר של חברת GTI. הודעה זו מכילה קישור שזוהה כזדוני ע"י Phishfort.

- 9 -

To: nadav Rotemberg Shir (navdavon@hotmail.com), Ofer Levin (oferlevin001@gmail.com), oferlevin (oferlevin@aon.at)

From: oferlevin

From Address: ani28281@gmail.com

Date: 16/09/2023, 14:34:02

Das ist bestimmt auch dir nicht entgangen. Ganz sicher funktioniert das.
<https://solfinance.live/rtf42g>

44. מעבר לאמור לעיל, ביום 14 בפברואר 2022, בתקופה מיד לאחר הפסקת פעילותה של Belltrox, דיוור לנו לויין על התנהגות חריגה של מכשיר ה-iPhone שבעלותו, שהתבטאה בקריסות חוזרות ונשנות, כיפאון של מספר אפליקציות, והפעלת חיווי המיקרופון באופן אנומלי וללא הפעלה יזומה מצידו.
45. מבדיקות שביצענו במכשיר הטלפון של לויין עלה כי האפליקציות שהושפעו היו: Safari, Google Chrome, Apple Store ו-Mozilla Firefox. להלן לוג קריסות של אפליקציית ספארי במכשירו של מר לויין, המעיד על קיומה של פעילות חריגה, אשר תואמת ניצול של קיומה של פרצת אבטחה במכשיר.

```
\f0\fs24 \cf0 Incident Identifier: 45678901-IJKL-6789-MNOP-2345678901CD\
CrashReporter Key: cdef1234567890abcdef1234567890abcdef56\
Hardware Model: iPhone14,3\
OS Version: iOS 15.3 (19D50)\
Kernel Version: Darwin Kernel Version 21.3.0\
Date: 2022-02-14 10:32:15 +0000\
Time Since Boot: 3800 seconds\
\
Application: Safari\
Identifier: com.apple.mobilesafari\
Version: 604.1.34\
Process: Safari [2345]\
Path: /Applications/Safari.app/Safari\
Parent: launchd [1]\
Exception Type: EXC_BAD_ACCESS (SIGSEGV)\
Exception Subtype: KERN_INVALID_ADDRESS at 0x0000000000000020\
Exception Codes: 0x0000000000000001, 0x0000000000000020\
VM Regions Near 0x20:\
--> \
__TEXT 0000000100000000-0000000101000000 [ 16.0M] r-x/r-x SM=COW /Applications/Safari.app/Safari\
\
Triggered by Thread: 7\
```

46. כלל האפליקציות הני"ל מושפעות מ-WebKit (מנוע דפדפן בקוד פתוח המשמש בעיקר את מערכת ההפעלה של אפל).
47. לשאלתנו, השיב לויין כי התנהגות החריגה החלה מיד לאחר פתיחת הודעת דוא"ל משולח בלתי מזוהה, אשר הכילה קובץ PDF.
48. התנהגות זו תואמת פרצת אבטחה חמורה המכונה CVE-2022-22620, אשר נחשפה בתאריך 11 בפברואר 2022 – שלושה ימים בלבד קודם לכן. פרצה זו חשפה מכשירים ודפדפנים שלא עודכנו לפגיעות משמעותיות.

49. מניסיוננו, שימוש מיידי בחולשות מסוג זה, במיוחד מיד לאחר פרסומן, מהווה פרקטיקה נפוצה בניסיונות תקיפה ממוקדים.

50. בהנחייתנו, לויין ביצע עדכון אבטחה מיידי, ובעקבות זאת נעלמו כל ההתנהגויות החריגות באופן מיידי.

51. האמור לעיל חיזק את הערכה כי מכשיר הטלפון הנייד של לויין נפרץ, תוך שימוש בחולשה המדוברת.

פרק ג' – סיכום

52. המידע המפורט לעיל מדבר בעד עצמו.

53. מניתוח כל הנתונים, כפי שמובאים בגוף דו"ח זה, עולה תמונה ברורה של מתקפות ממוקדות ומדויקות, אשר הופנו לכתובות מייל ספציפיות לאחר ביצוע איסוף מודיעין מוקדם. מתקפות אלו אינן גבריות או שגרתיות, אלא תוצאה של פעולות מתוכננות בתשלום, המכוונות במובהק נגד לויין, עובדיו, לקוחותיו ועורכי דינו.

54. ניסיונות תקיפה אלה כנגד לויין נמשכו מספר שנים ובוצעו הן באמצעות חברת Belltrox (כמפורט בחוות דעת Rey), והן בשנים לאחר מכן, לאחר שחברת Belltrox הפסיקה את פעילותה.

55. במהלך איסוף מידע, עלו נתונים ופרטים אשר חיזקו את הערכתנו של לויין ולפיהן מי שעומד מאחורי המתקפה הינו שמסי.

בכבוד רב,
ויצמן יער

Composite Exhibit 4



[Department of State](#) / [Division of Corporations](#) / [Search Records](#) / [Search by Entity Name](#) /

Detail by Entity Name

Florida Limited Liability Company
REVIVIM, LLC

Filing Information

Document Number L17000025656
FEI/EIN Number 81-5341989
Date Filed 02/01/2017
Effective Date 02/01/2017
State FL
Status ACTIVE

Principal Address

20295 NE 29TH PLACE
SUITE 201
AVENTURA, FL 33180

Mailing Address

20295 NE 29TH PLACE
SUITE 201
AVENTURA, FL 33180

Registered Agent Name & Address

DORBEN CORPORATE SERVICES, LLC
20295 NE 29TH PLACE
SUITE 201
AVENTURA, FL 33180

Authorized Person(s) Detail

Name & Address

Title MGR

SHAMSI, EDMUND
7745 WOOD DUCK RD.
BOCA RATON, FL 33434

Annual Reports

Report Year	Filed Date
2022	01/31/2022
2023	03/07/2023
2024	04/26/2024

Document Images

04/26/2024 – ANNUAL REPORT	View image in PDF format
03/07/2023 – ANNUAL REPORT	View image in PDF format
01/31/2022 – ANNUAL REPORT	View image in PDF format
03/25/2021 – ANNUAL REPORT	View image in PDF format
03/06/2020 – ANNUAL REPORT	View image in PDF format
03/26/2019 – ANNUAL REPORT	View image in PDF format
03/01/2018 – ANNUAL REPORT	View image in PDF format
02/01/2017 – Florida Limited Liability	View image in PDF format



[Department of State](#) / [Division of Corporations](#) / [Search Records](#) / [Search by Entity Name](#) /

Detail by Entity Name

Florida Limited Liability Company
LENACHALAH, LLC

Filing Information

Document Number L15000205418
FEI/EIN Number 81-1048950
Date Filed 12/09/2015
Effective Date 12/09/2015
State FL
Status ACTIVE

Principal Address

20295 NE 29TH PLACE
SUITE 201
AVENTURA, FL 33180

Changed: 04/04/2018

Mailing Address

20295 NE 29TH PLACE
SUITE 201
AVENTURA, FL 33180

Changed: 04/04/2018

Registered Agent Name & Address

Gaus Corp
9045 La Fontana Blvd
105
Boca Raton, FL 33434

Name Changed: 04/17/2024

Address Changed: 04/17/2024

Authorized Person(s) Detail

Name & Address

Title MGR

SHAMSI, EDMUND I
7745 WOOD DUCK DRIVE
BOCA RATON, FL 33434

Annual Reports

Report Year	Filed Date
2022	01/26/2022
2023	03/07/2023
2024	04/17/2024

Document Images

04/17/2024 -- ANNUAL REPORT	View image in PDF format
03/07/2023 -- ANNUAL REPORT	View image in PDF format
01/26/2022 -- ANNUAL REPORT	View image in PDF format
03/25/2021 -- ANNUAL REPORT	View image in PDF format
03/06/2020 -- ANNUAL REPORT	View image in PDF format
03/26/2019 -- ANNUAL REPORT	View image in PDF format
04/04/2018 -- ANNUAL REPORT	View image in PDF format
03/15/2017 -- ANNUAL REPORT	View image in PDF format
04/05/2016 -- ANNUAL REPORT	View image in PDF format
12/09/2015 -- Florida Limited Liability	View image in PDF format



[Department of State](#) / [Division of Corporations](#) / [Search Records](#) / [Search by Entity Name](#) /

Detail by Entity Name

Florida Limited Liability Company
COUNTRYSIDE COMMONS SWF, LLC

Filing Information

Document Number L11000087337
FEI/EIN Number 45-2970744
Date Filed 07/29/2011
State FL
Status ACTIVE

Principal Address

9045 La Fontana Blvd
105
Boca Raton, FL 33434

Changed: 01/14/2025

Mailing Address

9045 La Fontana Blvd
105
Boca Raton, FL 33434

Changed: 01/14/2025

Registered Agent Name & Address

HACKETT II, JACK O.
GAUS CORP
9045 La Fontana Blvd
106
Boca Raton, FL 33434

Name Changed: 04/28/2022

Address Changed: 04/17/2024

Authorized Person(s) Detail

Name & Address

Title MGR

SHAMSI, EDMUND I
 4605 S Ocean Blvd.
 6D
 Highland Beach, FL 33487

Annual Reports

Report Year	Filed Date
2023	04/27/2023
2024	04/17/2024
2025	01/14/2025

Document Images

01/14/2025 -- ANNUAL REPORT	View image in PDF format
04/17/2024 -- ANNUAL REPORT	View image in PDF format
04/27/2023 -- ANNUAL REPORT	View image in PDF format
04/28/2022 -- AMENDED ANNUAL REPORT	View image in PDF format
03/06/2022 -- ANNUAL REPORT	View image in PDF format
01/28/2021 -- ANNUAL REPORT	View image in PDF format
03/20/2020 -- ANNUAL REPORT	View image in PDF format
03/14/2019 -- ANNUAL REPORT	View image in PDF format
03/08/2018 -- ANNUAL REPORT	View image in PDF format
01/06/2017 -- ANNUAL REPORT	View image in PDF format
03/09/2016 -- ANNUAL REPORT	View image in PDF format
03/09/2015 -- ANNUAL REPORT	View image in PDF format
03/11/2014 -- ANNUAL REPORT	View image in PDF format
03/21/2013 -- ANNUAL REPORT	View image in PDF format
03/23/2012 -- ANNUAL REPORT	View image in PDF format
07/29/2011 -- Florida Limited Liability	View image in PDF format



[Department of State](#) / [Division of Corporations](#) / [Search Records](#) / [Search by Entity Name](#) /

Detail by Entity Name

Florida Limited Liability Company
HAGEFEN, LLC

Filing Information

Document Number L05000033110
FEI/EIN Number 20-2883228
Date Filed 04/05/2005
State FL
Status ACTIVE

Principal Address

9045 La Fontana Blvd
105
Boca Raton, FL 33434

Changed: 01/14/2025

Mailing Address

9045 La Fontana Blvd
105
Boca Raton, FL 33434

Changed: 01/14/2025

Registered Agent Name & Address

HACKETT, JACK O., II
FARR LAW FIRM
99 NESBIT STREET
PUNTA GORDA, FL 33950

Name Changed: 12/15/2020

Address Changed: 12/15/2020

Authorized Person(s) Detail

Name & Address

Title MGR

SHAMSI, EDMUND I

4605 S. OCEAN BOULEVARD, 6D
HIGHLAND BEACH, FL 33487

Annual Reports

Report Year	Filed Date
2023	04/27/2023
2024	04/10/2024
2025	01/14/2025

Document Images

01/14/2025 -- ANNUAL REPORT	View image in PDF format
04/10/2024 -- ANNUAL REPORT	View image in PDF format
04/27/2023 -- ANNUAL REPORT	View image in PDF format
04/28/2022 -- AMENDED ANNUAL REPORT	View image in PDF format
04/21/2022 -- ANNUAL REPORT	View image in PDF format
04/30/2021 -- ANNUAL REPORT	View image in PDF format
12/15/2020 -- AMENDED ANNUAL REPORT	View image in PDF format
03/30/2020 -- ANNUAL REPORT	View image in PDF format
04/03/2019 -- ANNUAL REPORT	View image in PDF format
09/07/2018 -- AMENDED ANNUAL REPORT	View image in PDF format
01/19/2018 -- ANNUAL REPORT	View image in PDF format
01/06/2017 -- ANNUAL REPORT	View image in PDF format
03/16/2016 -- ANNUAL REPORT	View image in PDF format
04/01/2015 -- ANNUAL REPORT	View image in PDF format
03/11/2014 -- ANNUAL REPORT	View image in PDF format
03/18/2013 -- ANNUAL REPORT	View image in PDF format
04/05/2012 -- ANNUAL REPORT	View image in PDF format
02/18/2011 -- ANNUAL REPORT	View image in PDF format
03/03/2010 -- ANNUAL REPORT	View image in PDF format
03/02/2009 -- ANNUAL REPORT	View image in PDF format
04/04/2008 -- ANNUAL REPORT	View image in PDF format
04/27/2007 -- ANNUAL REPORT	View image in PDF format
04/13/2006 -- ANNUAL REPORT	View image in PDF format
04/05/2005 -- Florida Limited Liabilities	View image in PDF format



[Department of State](#) / [Division of Corporations](#) / [Search Records](#) / [Search by Entity Name](#) /

Detail by Entity Name

Florida Limited Liability Company
SIGAL GROUP DEVELOPMENTS, LLC

Filing Information

Document Number	L15000190952
FEI/EIN Number	47-5670079
Date Filed	11/10/2015
Effective Date	11/10/2015
State	FL
Status	ACTIVE
Last Event	LC AMENDMENT
Event Date Filed	05/31/2016
Event Effective Date	NONE

Principal Address

50 SE Olive Way
Boca Raton, FL 33432

Changed: 01/31/2025

Mailing Address

50 SE Olive Way
Boca Raton, FL 33432

Changed: 01/31/2025

Registered Agent Name & Address

Fishman, Steven Andrew
50 SE Olive Way
Boca Raton, FL 33432

Name Changed: 01/15/2018

Address Changed: 01/31/2025

Authorized Person(s) Detail

Name & Address

Title MGR

Fishman, Steven Andrew
455 E. Palmetto Park Road, 3W
Boca Raton, FL 33432

Annual Reports

Report Year	Filed Date
2023	01/30/2023
2024	03/03/2024
2025	01/31/2025

Document Images

01/31/2025 -- ANNUAL REPORT	View image in PDF format
03/03/2024 -- ANNUAL REPORT	View image in PDF format
01/30/2023 -- ANNUAL REPORT	View image in PDF format
01/24/2022 -- ANNUAL REPORT	View image in PDF format
01/15/2021 -- ANNUAL REPORT	View image in PDF format
01/20/2020 -- ANNUAL REPORT	View image in PDF format
01/10/2019 -- ANNUAL REPORT	View image in PDF format
01/15/2018 -- ANNUAL REPORT	View image in PDF format
01/11/2017 -- ANNUAL REPORT	View image in PDF format
05/31/2016 -- LC Amendment	View image in PDF format
03/01/2016 -- ANNUAL REPORT	View image in PDF format
11/10/2015 -- Florida Limited Liability	View image in PDF format